

Colin R. Kass (*pro hac vice*)  
PROSKAUER ROSE LLP  
1001 Pennsylvania Ave., N.W.  
Washington, D.C. 20004  
(202) 416-6890  
ckass@proskauer.com

Robert C. Goodman (Bar No. 111554)  
Lauren Kramer Sujeeth (Bar No. 259821)  
ROGERS, JOSEPH, O'DONNELL, PC  
311 California Street, 10<sup>th</sup> Floor  
San Francisco, CA 94104  
(415) 956-2828  
rgoodman@rjo.com  
lsujeeth@rjo.com

*Attorneys for Defendant Bright Data Ltd.*  
*Additional counsel listed on signature page*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

X Corp.,

Plaintiff,

v.

BRIGHT DATA LTD.

Defendant

Case No. 23-cv-03698-WHA

Time: January 10, 2024, 8:00 AM

Court: Courtroom 12

Judge: Hon. William Alsup

**BRIGHT DATA'S MOTION TO DISMISS THE AMENDED COMPLAINT**

**NOTICE OF MOTION**

PLEASE TAKE NOTICE that the hearing on Bright Data's Motion to Dismiss the First Amended Complaint will take place on January 10, 2024, at 8:00 AM.

The motion seeks dismissal of X's tort claims (Count II-IV) for lack of personal jurisdiction and for failure to state a claim pursuant to Rules 12(b)(2) and (6). This motion also seeks dismissal of X's breach of contract claim (Count I) to the extent it rests on individual, non-defendant user accounts, and not accounts of Bright Data Ltd. pursuant to Rule 12(b)(6).

**STATEMENT OF ISSUES TO BE DECIDED**

1. Does the Court lack personal jurisdiction over X's tort claims because (i) the Terms' forum selection clause does not apply to claims that do not relate to any contract between Bright Data and X; and (ii) X failed to allege tortious conduct in or expressly aimed at California?

2. Does X's tortious interference claim fail under Rule 12(b)(6) because X has not alleged (i) the existence and breach of a valid and enforceable third-party contract, or (ii) any conduct that would constitute unlawful inducement of a breach?

3. Does X's unjust enrichment claim fail under Rule 12(b)(6) because X has not alleged (i) a claim arising independent of the X Terms of Service, or (ii) any independent (non-contractual) property right to prevent Bright Data from engaging in public web search?

4. Does X's trespass claim fail under Rule 12(b)(6) because (i) an internet user does not commit trespass by searching the public web; and (ii) a website operator does not suffer injury when it receives communication requests from other internet users?

5. Does X's misappropriation claim fail under Rule 12(b)(6) because X does not own either the Internet or public Internet data?

6. Does X's unfair competition claim fail under Rule 12(b)(6) because X has not alleged any unfair method of competition or violation of any other law?

7. Does X's breach of contract claim based on individual employee accounts fail under Rule 12(b)(6) because Bright Data is not a party to the contract sued upon?

## TABLE OF CONTENTS

I.	INTRODUCTION. ....	1
II.	FACTUAL BACKGROUND. ....	3
III.	THE COURT LACKS PERSONAL JURISDICTION OVER X’S TORT CLAIMS. ....	4
A.	Bright Data Did Not Waive Personal Jurisdiction over X’s Tort Claims. ....	5
1.	X’s Tortious Interference Claim Depends on X’s Contracts with Third Parties, Not Bright Data. ....	6
2.	X’s Other Tort Claims Do Not Arise Under or Relate to the Now Terminated and Rejected Terms. ....	8
B.	X Has Not Plausibly Alleged Specific Personal Jurisdiction. ....	8
1.	X Cannot Base Specific Jurisdiction on X’s Own Domicile. ....	9
2.	X Cannot Base Specific Jurisdiction on the Alleged Existence of Bright Data’s Sales Office or the Location of Certain Employees. ....	9
3.	X Cannot Base Specific Jurisdiction on Bright Data’s Sale of General-Purpose Scraping Services. ....	10
4.	The Conclusory Allegation that Bright Data “Targeted” X’s California Users Does Not Establish Specific Jurisdiction. ....	14
IV.	X FAILS TO STATE A CLAIM FOR TORTIOUS INTERFERENCE. ....	15
A.	X Fails to Allege Breach of any Valid and Enforceable Third-Party Contract. ....	15
B.	Offering a Lawful Service is Not Inducement. ....	18
V.	X FAILS TO STATE A CLAIM FOR UNJUST ENRICHMENT. ....	19
VI.	X FAILS TO STATE A CLAIM FOR TRESPASS TO CHATTELS. ....	22
A.	Public Internet Search Does Not Constitute a Trespass. ....	23
B.	X Fails to Allege Intentional Interference with Its Property. ....	25
C.	X Fails to Allege that Any Interference with Its Servers Has Been Substantial. ....	27
VII.	X FAILS TO STATE A CLAIM FOR MISAPPROPRIATION. ....	29

VIII.	X FAILS TO STATE A CLAIM UNDER THE UCL. ....	31
IX.	X’S INDIVIDUAL USER ACCOUNT CLAIMS SHOULD BE DISMISSED. ....	33
X.	CONCLUSION.....	35

**TABLE OF AUTHORITIES<sup>1</sup>****Page(s)****CASES**

<i>123 Los Robles LLC v. Metzler</i> , 2017 WL 10311210 (C.D. Cal. 2017).....	27
<i>Adobe Sys.Inc. v. Nwubah</i> , 2019 WL 6611096 (N.D. Cal. 2019) .....	13
<i>Alexander v. Metro-Goldwyn-Mayer Studios Inc.</i> , 2017 WL 5633407 (C.D. Cal. 2017).....	29
<i>Androutsakos v. M/V PSARA</i> , 2004 WL 1305802 (D. Or. 2004).....	5
<i>Astiana v. Hain Celestial Grp., Inc.</i> , 783 F.3d 753 (9th Cir. 2015) .....	20
<i>Aviation All. Ins. Risk Retention Grp., Inc. v. Polaris Enter. Grp., Inc.</i> , 2017 WL 2799151 (D. Mont. 2017) .....	6
<i>Avila v. Citrus Cnty. Coll. Dist.</i> , 38 Cal. 4th 148 (Cal. 2006).....	24
<i>Barclays Cap. Inc. v. Theflyonthewall.com, Inc.</i> , 650 F.3d 876 (2d Cir. 2011).....	30
<i>Berrett v. Life Ins. Co. of SW</i> , 623 F. Supp. 946 (D.Utah 1985).....	7
<i>Blizzard Ent. Inc. v. Ceiling Fan Software LLC</i> , 28 F. Supp. 3d 1006 (C.D. Cal. 2013) .....	18
<i>BNSF Ry. Co. v. Tyrrell</i> , 581 U.S. 402 (2017).....	8
<i>Briskin v. Shopify, Inc.</i> , 2023 WL 8225346 (9th Cir. 2023) .....	<i>passim</i>
<i>Bristol-Myers Squibb Co. v. Superior Court</i> , 582 U.S. 255 (2017).....	9, 11, 14

---

<sup>1</sup> Unless otherwise specified, all emphasis added, initial capitalizations conformed without brackets, and internal citations and quotation marks omitted.

1	<i>Cap. Credit All., Inc. v. Lowpay, Inc.</i> ,	
2	2008 WL 2513692 (D. Nev. 2008) .....	29
3	<i>Carroll v. J.M. Smucker Co.</i> ,	
4	2023 WL 4053796 (N.D. Cal. 2023) (Alsup, J.).....	11, 15
5	<i>Casillas v. Berkshire Hathaway Homestate Ins. Co.</i> ,	
6	79 Cal. App. 5th 755 (2022) .....	27
7	<i>Chang v. Virgin Mobile USA, LLC</i> ,	
8	2009 WL 111570 (N.D. Tex. 2009).....	13
9	<i>Coal. for ICANN Transparency Inc. v. VeriSign, Inc.</i> ,	
10	452 F. Supp. 2d 924 (N.D. Cal. 2006) .....	6
11	<i>Cole-Parmer Instrument Co., LLC v. Prof. Lab's</i> ,	
12	2021 WL 3053201 (N.D. Cal. 2021) .....	5
13	<i>Cont'l Appliances, Inc. v. Thomas</i> ,	
14	2012 WL 3646887 (N.D. Cal. 2012) .....	8, 9
15	<i>CZ Servs., Inc. v. Express Scripts Holding Co.</i> ,	
16	2018 WL 3972030 (N.D. Cal. 2018) .....	6
17	<i>Diversified Metal Distribs., LLC v. AK Steel Corp.</i> ,	
18	2007 WL 403870 (E.D. Ky. 2007) .....	6
19	<i>Doe v. Geller</i> ,	
20	533 F. Supp. 2d 996 (N.D. Cal. 2008) .....	13
21	<i>eBay, Inc. v. Bidder's Edge, Inc.</i> ,	
22	100 F. Supp. 2d 1058 (N.D. Cal. 2000) .....	25
23	<i>ESG Cap. Partners, LP v. Stratos</i> ,	
24	828 F.3d 1023 (9th Cir. 2016) .....	20
25	<i>Gannett Satellite Info. Network, Inc. v. Rock Valley Cmty. Press, Inc.</i> ,	
26	1994 WL 606171 (N.D. Ill. 1994) .....	30
27	<i>GemCap Lending I, LLC v. Bateman</i> ,	
28	2017 WL 8183191 (C.D. Cal. 2017).....	6
	<i>Genesco, Inc. v. T. Kakiuchi &amp; Co.</i> ,	
	815 F.2d 840 (2d Cir. 1987).....	6
	<i>Goodyear Dunlop Tires Operations, S.A. v. Brown</i> ,	
	564 U.S. 915 (2011).....	8, 9
	<i>Green Crush LLC v. Paradise Splash I, Inc.</i> ,	
	2018 WL 4940825 (C.D. Cal. 2018).....	16

1	<i>Hanson v. Denckla,</i>	
2	357 U.S. 235 (1958).....	11
3	<i>hiQ Labs, Inc. v. LinkedIn Corp.,</i>	
4	2021 WL 1531172 (N.D. Cal. 2021) .....	31
5	<i>Hodsdon v. Mars, Inc.,</i>	
6	891 F.3d 857 (9th Cir. 2018) .....	33
7	<i>Hollywood Screentest of Am., Inc. v. NBC Universal, Inc.,</i>	
8	151 Cal. App. 4th 631 (2007) .....	29
9	<i>Hunt v. Zuffa, LLC,</i>	
10	361 F. Supp. 3d 992 (D. Nev. 2019).....	24
11	<i>ICC LLC v. WhatsApp Inc.,</i>	
12	2013 WL 5230631 (E.D. Va. 2013).....	13
13	<i>In re Charles Schwab Corp. Sec. Litig.,</i>	
14	257 F.R.D. 534 (N.D. Cal. 2009) (Alsup, J.).....	15, 16
15	<i>In re Orange, S.A.,</i>	
16	818 F.3d 956 (9th Cir. 2016) .....	5
17	<i>Ingenieria Alimentaria Del Matatipac, S.A. de C.V. v. Ocean Garden Prods. Inc.,</i>	
18	320 F. App'x 548 (9th Cir. 2009) .....	6
19	<i>Intel Corp. v. Hamidi,</i>	
20	30 Cal.4th 1342 (2003) .....	25, 27, 28
21	<i>Karlberg European Tanspa, Inc. v. JK-Josef Kratz Vertriebsgesellschaft MbH,</i>	
22	699 F. Supp. 669 (N.D. Ill. 1988) .....	6
23	<i>Kearns v. Ford Motor Co.,</i>	
24	567 F.3d 1120 (9th Cir. 2009) .....	32
25	<i>Kendig v. N. Tier Energy LP,</i>	
26	2017 WL 6001435 (D. Ariz. 2017).....	6
27	<i>Knight v. Jewett,</i>	
28	3 Cal. 4th 296 (1992) .....	23, 24
	<i>Low v. LinkedIn Corp.,</i>	
	900 F. Supp. 2d 1010 (N.D. Cal. 2012) .....	19, 20
	<i>Man-D-Tec, Inc. v. Nylube Prods. Co., LLC,</i>	
	2012 WL 1831521 (D. Ariz. 2012).....	13
	<i>Manetti- Farrow, Inc. v. Gucci Am., Inc.,</i>	
	858 F.2d 509 (9th Cir. 1988) .....	5

1	<i>Matus v. Premium Nutraceuticals, LLC,</i>	
2	715 F. App'x 662 (9th Cir. 2018) .....	11, 12
3	<i>McBride v. Boughton,</i>	
4	123 Cal. App. 4th 379 (2004) .....	20
5	<i>Mediterranean Enters., Inc. v. Ssangyong Corp.,</i>	
6	708 F.2d 1458 (9th Cir. 1983) .....	5
7	<i>Mishiyev v. Alphabet, Inc.,</i>	
8	444 F. Supp. 3d 1154 (N.D. Cal. 2020) (Alsup, J.) .....	15
9	<i>Nat'l Basketball Ass'n v. Motorola, Inc.,</i>	
10	105 F.3d 841 (2d Cir.1997).....	30
11	<i>Nevada DeAnza Fam. Ltd. P'ship v. Tesoro Re. &amp; Mktg. LLC,</i>	
12	474 F. Supp. 3d 1087 (N.D. Cal. 2020) .....	18
13	<i>Nexsales Corp. v. Salebuild, Inc.,</i>	
14	2012 WL 216260 (N.D. Cal. 2012) .....	29
15	<i>Nguyen v. Barnes &amp; Noble Inc.,</i>	
16	763 F.3d 1171 (9th Cir. 2014) .....	16
17	<i>Nunes v. Twitter, Inc.,</i>	
18	103 Va. Cir. 184 (Cir. Ct. 2019) .....	7
19	<i>Olney v. Job.com, Inc.,</i>	
20	2014 WL 4660851 (E.D. Cal. 2014).....	17
21	<i>Orchard Supply Hardware LLC v. Home Depot USA, Inc.,</i>	
22	967 F. Supp. 2d 1347 (N.D. Cal. 2013) .....	17
23	<i>Picot v. Weston,</i>	
24	780 F.3d 1206 (9th Cir. 2015) .....	12
25	<i>Price v. Apple, Inc.,</i>	
26	2022 WL 1032462 (N.D. Cal. 2022) .....	23
27	<i>Ramondetta v. Philips Elecs. Ltd.,</i>	
28	2007 WL 4209443 (N.D. Cal. 2007) .....	4, 5
	<i>Ray v. Experian,</i>	
	2007 WL 4245459 (N.D. Tex. 2007).....	13
	<i>Revitch v. DirecTV, LLC,</i>	
	2018 WL 4030550 (N.D. Cal. 2018) .....	7
	<i>Reynolds v. Binance Holdings Ltd.,</i>	
	481 F. Supp. 3d 997 (N.D. Cal. 2020) .....	5



1	<i>San Miguel v. HP Inc.,</i>	
2	317 F. Supp. 3d 1075 (N.D. Cal. 2018) .....	16
3	<i>Schentag v. Nebgen,</i>	
4	2018 WL 3104092 (S.D.N.Y. 2018) .....	11
5	<i>Schulz v. Cisco WebEx, LLC,</i>	
6	2014 WL 2115168 (N.D. Cal. 2014) .....	8
7	<i>Schwarzenegger v. Fred Martin Motor Co.,</i>	
8	374 F.3d 797 (9th Cir. 2004) .....	4, 5
9	<i>Sebastian Int'l, Inc. v. Russolillo,</i>	
10	162 F. Supp. 2d 1198 (C.D. Cal.) .....	18
11	<i>Smith v. Facebook, Inc.,</i>	
12	262 F. Supp. 3d 943 (N.D. Cal. 2017) .....	12
13	<i>Soil Retention Prods., Inc. v. Brentwood Indus., Inc.,</i>	
14	521 F. Supp. 3d 929 (S.D. Cal. 2021) .....	15, 16
15	<i>Swartz v. KPMG LLP,</i>	
16	476 F.3d 756 (9th Cir. 2007) .....	14
17	<i>Synopsys, Inc. v. Ubiquiti Networks, In.,</i>	
18	313 F. Supp 3d 1056 (N.D. Cal. 2018) .....	27
19	<i>Ticketmaster Corp. v. Tickets.com, Inc.,</i>	
20	2 F. App'x 741 (9th Cir. 2001) .....	28
21	<i>Ticketmaster Corp. v. Tickets.com, Inc.,</i>	
22	2000 WL 1887522 (C.D. Cal. 2000), <i>aff'd</i> , 2 F. App'x 741 (9th Cir. 2001) .....	28
23	<i>Ticketmaster L.L.C. v. RMG Techs.,</i>	
24	2007 WL 2989504 (C.D. Cal. 2007) .....	18
25	<i>Twitter, Inc. v. Taamneh,</i>	
26	598 U.S. 471 (2023) .....	2, 18, 19
27	<i>UMG Recordings, Inc. v. Glob. Eagle Ent., Inc.,</i>	
28	117 F. Supp. 3d 1092 (C.D. Cal. 2015) .....	16
	<i>United States Golf Assn. v. Arroyo Software Corp.,</i>	
	69 Cal. App. 4th 607 (1999) .....	29
	<i>Vertkin v. Vertkin,</i>	
	2007 WL 4287512 (N.D. Cal. 2007) .....	27
	<i>Volkswagen Grp. of Am., Inc. v. Smartcar, Inc.,</i>	
	2022 WL 20184651 (N.D. Cal. 2022) .....	27

1	<i>Walden v. Fiore</i> ,	
2	571 U.S. 277 (2014).....	9
3	<i>Welenco, Inc. v. Corbell</i> ,	
4	2013 WL 5423100 (E.D. Cal. 2013).....	5, 7
5	<i>Wexler v. AT&amp;T Corp.</i> ,	
6	211 F. Supp. 3d 500 (E.D.N.Y. 2016) .....	7
7	<i>WhatsApp, Inc. v. NSO Grp. Techs. Ltd.</i> ,	
8	472 F. Supp. 3d 649 (N.D. Cal. 2020) .....	26, 28
9	<i>White Buffalo Ventures, LLC v. Univ. of Texas at Austin</i> ,	
10	420 F.3d 366 (5th Cir. 2005) .....	28
11	<i>Woods v. Google Inc.</i> ,	
12	2011 WL 3501403 (N.D. Cal. 2011) .....	32
13	<i>Yan Guo v. Kyani, Inc.</i> ,	
14	311 F. Supp. 3d 1130 (C.D. Cal. 2018) .....	7
15	<i>Yei A. Sun v. Advanced China Healthcare, Inc.</i> ,	
16	901 F.3d 1081 (9th Cir. 2018) .....	6
17	<b>STATUTES</b>	
18	Cal. Bus. & Prof. Code § 17200 .....	31
19	<b>RULES</b>	
20	Fed. R. Civ. P. 12.....	<i>passim</i>
21	<b>OTHER AUTHORITIES</b>	
22	Eric J. Feigin, <i>Architecture of Consent: Internet Protocols and Their Legal</i>	
23	<i>Implication</i> , 56 Stan. L. Rev. 901 (2004) .....	23
24	Restatement (First) of Restitution.....	22
25	Restatement (Second) of Contracts.....	20, 22
26	Restatement (Second) of Torts.....	<i>passim</i>
27	Restatement (Third) Of Agency .....	34, 35
28		

## I. INTRODUCTION.

The public has a right to search public information. Seems like a basic, even universal, human right. But X says no. It says it controls its corner of the Internet. But this case does not concern any proprietary or confidential information. Twitter, now X, bills itself as a public town square, telling users – in the very contracts sued upon – that, by tweeting, they are “directing [X] to disclose [their] information as broadly as possible.” Ex. 2 § 3.1. This information is “public by default” and “available for viewing by the *general public*.” *Id.*; Ex. 3. X admits that “*the public does not need to be signed in to view [this] content.*” Ex. 2 § 3.1. Nor does X assert any copyright or property interest in this information. It is also data X decided not to protect under the Computer Fraud and Abuse Act by putting it behind a log-in screen. Instead, X seeks to exert control over this *public domain information* through contract. This case tests the strength of those contracts.

X first sues under contract. It says that, because Bright Data opened a (now *terminated*) corporate account to advertise its lawful services, Bright Data is contractually prohibited from scraping public data on X’s site, even if the account was never used for that purpose. X also brings a panoply of tort claims, attempting to fill the void left by the terminated contract, and to attack Bright Data for providing services that *unidentified* customers, who may or may not have X accounts, *might* have used to scrape this same public data. This motion focuses primarily on tort, saving contract for another day.<sup>2</sup>

Two fundamental principles guide this motion. *First*, collecting public information online is not illegal, and doing so, or offering lawful services for others to do so, does not subject a service provider to personal jurisdiction in California. *Second*, surfing the public web does not impinge a website operator’s property, particularly when the operator does not own the information it hosts.

The first principle resolves tortious interference. A simple example illustrates: Alice lives in Florida and sells hand-crafted pens on Etsy. Bob, a California resident, buys a pen and uses it

---

<sup>2</sup> Because the Amended Complaint (“FAC”, ECF 36) does not allege that Bright Data’s accounts have been terminated, we leave the effect of such termination on X’s forward-looking claims for subsequent motion practice. Due to the issue’s importance, and lack of disputed material facts, Bright Data intends to request expedited motion practice on this issue at the Initial Case Management Conference.

1 to sign a check that violates his contract with Chris, another California resident. Chris sues Alice  
2 for tortious interference, claiming Alice knew or should have foreseen the possibility that Bob  
3 would use the pen to breach his contract. Chris’s claim fails both because selling a lawful product  
4 is not unlawful inducement, unless Alice was somehow “certain or substantially certain” the pen  
5 would be used for illicit purposes, and because the court lacks personal jurisdiction over Alice  
6 since she did not engage in any tortious activity in, or expressly aimed at, California. *See*  
7 Restatement (Second) of Torts, § 766, cmt. j; *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023).

8 X’s tortious interference claim fails for the same reasons. Bright Data (Alice, in this  
9 example) offers lawful proxy and scraping services (the pen) to customers across the globe.  
10 Though not actually alleged, X speculates that some unidentified users of unknown location  
11 (hypothetical Bobs) potentially use those services in violation of X’s (Chris’s) contractual rights.  
12 Even if that were so, there is still no inducement and no tortious conduct in California. So, there  
13 is neither claim nor jurisdiction, regardless of whether X can show a California Bob.

14 This simple **legal** principle compels dismissal of X’s tortious interference claim. There is  
15 no general jurisdiction over Bright Data, an Israeli company. X seeks to overcome this by asserting  
16 that Bright Data once opened an account with a California forum selection clause. But the forum  
17 clause does not cover tortious interference because the claim is premised on a breach of *third-party*  
18 contracts, not any contract with Bright Data. X gets no further with Bright Data’s alleged  
19 California contacts. The only *conduct* alleged is Bright Data’s sale of scraping tools and services  
20 to some unidentified customers around the world, some of whom may happen to be in California.  
21 But because the sale of these services is not *ipso facto* an inducement to breach, there is no  
22 “intentional act” in or aimed at California. In a controlling decision of first impression, the Ninth  
23 Circuit just held, “[w]hen a company operates a **nationally available e-commerce payment**  
24 **platform** and is indifferent to the location of end-users, the extraction and retention of consumer  
25 data [the alleged unlawful activity], without more, does not subject the defendant to specific  
26 jurisdiction in the forum where the online purchase was made.” *Briskin v. Shopify, Inc.*, 2023 WL  
27 8225346, \*1 (9th Cir. 2023). That precludes personal jurisdiction over X’s tort claims.

1 A second principle undergirding this motion – that surfing the public web does not interfere  
 2 with any property right – defeats X’s remaining tort claims. The Internet is a global  
 3 communications network. It is founded on, and depends on, openness and access. Anyone with a  
 4 server or a computer can access the internet and can use it to communicate with everyone else who  
 5 has done so. That a particular server request may be unwelcome – like an unwanted telephone call  
 6 in the days of yore –does not make it illegal. It does not mean that there has been a trespass,  
 7 misappropriation, or unfair use of the communications network. By connecting its servers to the  
 8 Internet, X invited digital requests from all comers. That is all Bright Data, and its customers, did;  
 9 and per the rules of the Internet, X’s servers responded with information X chose to make publicly  
 10 available. There is no tort in sight. X’s claims must be dismissed.

## 11 **II. FACTUAL BACKGROUND.**

12 The Internet is the largest public repository of information ever assembled. Though  
 13 theoretically accessible to anyone with internet access, sheer volume makes much of the data  
 14 inaccessible. It is a problem of information overload. Google – the largest scraper on the planet  
 15 – helped solve part of that problem. Its bots crawl millions of websites, including X’s. When  
 16 users type a query, Google searches its vast databases and identifies the most relevant websites.  
 17 Google revolutionized the Internet.

18 Bright Data is also revolutionizing the Internet. Its suite of technologies and services help  
 19 Fortune 500 companies, academic institutions, and small businesses retrieve and synthesize vast  
 20 amounts of *public* information. While Google curates a collection of links, Bright Data creates  
 21 datasets and helps customers create their own. FAC ¶¶ 45, 50-62. This is a good thing.

22 Shortly after Elon Musk purchased Twitter and changed its name to X, however, X sued to  
 23 prevent Bright Data and its customers from scraping *public* information users posted to X. X does  
 24 not claim any copyright or other ownership interest in this information. As X tells users: “You  
 25 retain your rights to any Content you submit, post or display on or through the Services. What’s  
 26 yours is yours — *you own your Content.*” See Ex. 1 § 3. This information is “*public by default.*”<sup>3</sup>  
 27

28 <sup>3</sup> Because X’s privacy policy is expressly incorporated into the Terms (which in turn is

Ex. 3 at 1. Because X “primarily [is] designed to help [users] share information with the world,” when users post information, they are “directing [X] to disclose that information as *broadly as possible*,” making the information “available for viewing by the *general public*” and for collection by “*Internet search engines*” who have scraped the data. Ex. 2 § 3.1; *see* Ex. 3 at 3. Importantly, “*the public does not need to be signed in* to view” this content. Ex. 2 § 3.1. That is, a person must have an account to *post* content, *see* FAC ¶ 20, but anyone can *access* it.

Bright Data makes this *public* information more accessible. Bright Data generally offers three types of services: datasets, scraping tools, and proxy network services. FAC ¶¶ 50-51, 55-58, 63-64. These services, as X admits, have an infinite variety of uses, most having nothing to do with X. For example, they can be used to “anonymously” search the web, or to scrape publicly available information on e-commerce sites, such as Amazon, or “other platforms,” such as Facebook or Instagram. *Id.* ¶¶ 6, 50. X does not allege that any of these uses violates X’s rights.

In asserting contract and various torts, X focuses on one use case. To create and maintain its service, X made the unilateral decision to connect its servers to the Internet and invite anyone, anywhere, to access its content. It chose not to place vast quantities of this content behind a log-in screen. But X does not allege that Bright Data, its services, or its customers scraped non-public data or used any X account to scrape this information. This case is about public information. *See id.* ¶ 45(c) (use “the latest data collection techniques to scrape, structure, and analyze *public* web data.”); ¶ 50, Figure 7 (“Tap into Twitter *public* accounts”); ¶ 56, Figure 9 (“you can start scraping Twitter *public* data using our Web Scraper IDE.”); ¶ 58, Figure 10 (“scrape data ... from *public* Twitter profiles”); ¶ 64 (use Bright Data’s proxy network to “gather vast amounts of *public* web data.”).

### III. THE COURT LACKS PERSONAL JURISDICTION OVER X’S TORT CLAIMS.

X “bears the burden of demonstrating personal jurisdiction for each separate claim.” *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004); *Ramondetta v.*

incorporated into the Complaint), it is properly considered on a motion to dismiss.

1 *Philips Elecs. Ltd.*, 2007 WL 4209443, \*2 n.3 (N.D. Cal. 2007) (same).<sup>4</sup> For each tort, X offers  
 2 two grounds: waiver via the Terms’ forum selection clause and minimum contacts. Neither works.

3 **A. *Bright Data Did Not Waive Personal Jurisdiction over X’s Tort Claims.***

4 X invokes the Terms’ forum selection clause, which requires users to “consent[] to personal  
 5 jurisdiction in California” for “disputes related to the Terms.” FAC ¶ 8. But X’s tort claims do  
 6 not relate to any contract between Bright Data and X. Its tortious inference claim involves  
 7 contracts between X and *third-parties* across the globe. Bright Data did not consent to litigate that  
 8 conduct here. Similarly, X’s other tort claims – trespass, misappropriation, and unfair competition  
 9 claims – presuppose the *absence* of any contractual relationship. That is fatal to any claim of  
 10 contractual waiver.

11 “Whether a forum selection clause applies to tort claims depends on whether resolution of  
 12 the claims relates to interpretation of the contract.” *Manetti- Farrow, Inc. v. Gucci Am., Inc.*, 858  
 13 F.2d 509, 514 (9th Cir. 1988); *In re Orange, S.A.*, 818 F.3d 956, 962 (9th Cir. 2016) (clause  
 14 covering “[a]ny and all” claims “arising out of or relating” to the agreement does not apply to  
 15 claim that defendant hacked plaintiff’s computers because it involved the breach of different  
 16 agreements and torts that did not require “interpretation” of the contract).<sup>5</sup>

17 This standard asks whether the alleged tort “*could have been accomplished even if the*  
 18 *Agreement did not exist.*” *Mediterranean Enters., Inc. v. Ssangyong Corp.*, 708 F.2d 1458, 1464  
 19 (9th Cir. 1983); *Genesco, Inc. v. T. Kakiuchi & Co.*, 815 F.2d 840, 856 (2d Cir. 1987) (following  
 20

---

21 <sup>4</sup> This is a facial challenge. *Cole-Parmer Instrument Co., LLC v. Prof. Lab’s*, 2021 WL 3053201,  
 22 \*7 (N.D. Cal. 2021) (“It is the plaintiff’s burden to plead allegations” to support personal  
 23 jurisdiction.); *Reynolds v. Binance Holdings Ltd.*, 481 F. Supp. 3d 997, 1005 (N.D. Cal. 2020)  
 24 (applying *Twombly* to personal jurisdiction allegations). If the Complaint survives a facial  
 challenge, Bright Data will assert any further factual challenge in its Answer, preserving the  
 defense for trial. See Fed. R. Civ. P. 12(h)(1)(B)(ii).

25 <sup>5</sup> *Manetti-Farrow* established a general test that does not depend on the specific text of the clause.  
 26 See *Androutsakos v. M/V PSARA*, 2004 WL 1305802, \*6 (D. Or. 2004) (“the [*Manetti-Farrow*]  
 27 court announced a more general rule for determining whether a forum selection clause applies ...,  
 28 declar[ing] that a forum selection clause applies to tort claims if resolution of the claims relates to  
 interpretation of the contract.”); *Welenco, Inc. v. Corbell*, 2013 WL 5423100, \*7 (E.D. Cal. 2013)  
 (“the *Manetti-Farrow* test is not limited to the clause at issue in that case”).



*Mediterranean*, and concluding that tortious interference claims do “not arise under or relate to [the parties’] sales agreements”); *Yei A. Sun v. Advanced China Healthcare, Inc.*, 901 F.3d 1081, 1086 (9th Cir. 2018) (claim must have a “**logical or causal connection** to the agreement”). If the claim “will stand or fall without any reference to the agreements,” the forum selection does not apply. *CZ Servs., Inc. v. Express Scripts Holding Co.*, 2018 WL 3972030, \*2 (N.D. Cal. 2018); *Kendig v. N. Tier Energy LP*, 2017 WL 6001435, \*4 (D. Ariz. 2017) (distinguishing claims the plaintiff “would have been entitled to pursue” “even if the [parties] had never executed” a contract, and claims that are “**entirely dependent** on the existence” of the contract). Since X’s tort claims do not depend on the existence or interpretation of any contract between Bright Data and X, the forum selection clause does not apply.

**1. X’s Tortious Interference Claim Depends on X’s Contracts with Third Parties, Not Bright Data.**

By definition, tortious interference involves a third-party contract, not one between a plaintiff and defendant. Thus, the claim does not relate to, arise out of, or depend on Bright Data’s alleged acceptance of the Terms. Because X’s tortious interference claim is not “dependent on rights or duties created by the [parties’] agreement[,]” Bright Data has not waived personal jurisdiction. *See Karlberg European Tanspa, Inc. v. JK-Josef Kratz Vertriebsgesellschaft MbH*, 699 F. Supp. 669, 672 (N.D. Ill. 1988).<sup>6</sup>

The Terms’ express language reinforces this conclusion. *First*, the Terms are limited to a

---

<sup>6</sup> *See also, e.g., Ingenieria Alimentaria Del Matatipac, S.A. de C.V. v. Ocean Garden Prods. Inc.*, 320 F. App’x 548, 549–50 (9th Cir. 2009) (“district court ... abused its discretion” in applying forum selection clause to “interference [claims because they] do not relate to interpretation of the contracts”); *Coal. for ICANN Transparency Inc. v. VeriSign, Inc.*, 452 F. Supp. 2d 924, 931-32 (N.D. Cal. 2006) (forum selection clause covering claims “relating to” the parties’ agreement does not include tortious interference); *GemCap Lending I, LLC v. Bateman*, 2017 WL 8183191, \*5 (C.D. Cal. 2017) (tort claims not covered because plaintiffs “present no argument on how resolution of their tort claims requires interpreting the [parties’] agreements”); *Aviation All. Ins. Risk Retention Grp., Inc. v. Polaris Enter. Grp., Inc.*, 2017 WL 2799151, \*4 (D. Mont. 2017) (arbitration provision inapplicable to claim “based on interference with **third party contracts**, not the [parties’] Agreement.”); *Diversified Metal Distribs., LLC v. AK Steel Corp.*, 2007 WL 403870, \*2 (E.D. Ky. 2007) (“Plaintiff’s tortious interference claim clearly does not relate to the agreement between the parties...”).



1 user's own "use" of X. *See* Ex. 1 at 3-4, 12 (the Terms "govern **your** access to and use of our ...  
2 'Services' ... and ... 'Content'"). Because X's tortious interference claim relates to third-parties'  
3 access or use, it is not covered. *Wexler v. AT&T Corp.*, 211 F. Supp. 3d 500, 504 (E.D.N.Y. 2016)  
4 ("no reasonable person would think that checking a box accepting the 'terms and conditions'  
5 necessary to [create a user account] would obligate them to [litigate] literally every possible dispute  
6 he or she might have with the service provider [in California].... Rather, a reasonable person  
7 would be expressing, at most, an intent to agree to [litigate] disputes connected in some way to the  
8 service agreement."); *Revitch v. DirecTV, LLC*, 2018 WL 4030550, \*14 (N.D. Cal. 2018) (same);  
9 *Yan Guo v. Kyani, Inc.*, 311 F. Supp. 3d 1130, 1141 (C.D. Cal. 2018) (claims "outside of what ...  
10 was contemplated by [the] agreement ... are not within the scope of the forum selection clause.").

11 *Second*, X's forum selection clause applies only to disputes "related to the[] Terms or the  
12 Services" provided under the contract. Ex. 1 § 6. This does not reach tortious interference related  
13 to third-party contracts, and use or access of X. *See Berrett v. Life Ins. Co. of SW*, 623 F. Supp.  
14 946, 948-49 (D. Utah 1985) ("It is highly unlikely that ... the parties contemplated that tort claims"  
15 involving "acts [] unrelated to the interpretation of the agency agreement" would be covered by  
16 the forum selection clause); *Welenco*, 2013 WL 5423100, \*7 (forum selection inapplicable to claim  
17 that the defendant "acted in concert" with entities that "improperly accessed" plaintiffs' "computer  
18 system" because the claim "arise[s] from the relationship between [the plaintiff and the third  
19 parties,] not from the relationship between [the plaintiff and defendant].").

20 *Nunes v. Twitter, Inc.*, 103 Va. Cir. 184, 186 (Cir. Ct. 2019), is particularly instructive.  
21 There, plaintiffs sued Twitter for publishing defamatory statements posted by third-party users. In  
22 rejecting Twitter's argument that the "Plaintiff [had] twitter accounts and [was] therefore subject  
23 to the [California forum selection clause]," the court explained that the Terms do "not apply" to  
24 plaintiffs' claims because they do not arise out of plaintiffs' own "use of twitter." *Id.* As the Court  
25 noted, the plaintiff would still have a claim even if it "did not have [any] twitter account." *Id.* So  
26 too here. The existence of a Bright Data X account is irrelevant to tortious interference. As such,  
27 the forum selection clause does not govern X's tortious interference claim.  
28

2. ***X's Other Tort Claims Do Not Arise Under or Relate to the Now Terminated and Rejected Terms.***

X's other tort claims also do not arise from, or relate to, any contract with Bright Data. X amended its Complaint to assert such claims only after Bright Data terminated its X account, eliminating any forward-looking contractual relationship. Without a contract, there can be no contractual jurisdictional waiver. Nor does the forum selection clause cover X's past tort claims. Unjust enrichment presupposes the absence of contract because a "plaintiff may not plead ... an enforceable contract and maintain a quasi-contract claim [for unjust enrichment] at the same time." *Schulz v. Cisco WebEx, LLC*, 2014 WL 2115168, \*5 (N.D. Cal. 2014). As for the UCL, X asserts that Bright Data provided proxy services allowing anonymous search. That has nothing to do with the Terms. X's trespass and misappropriation claims are premised on the notion that Bright Data accessed (or "trespassed") on X's servers and collected (or "misappropriated") public data. But neither X nor Bright Data assert that any *contract* is the source of consent for the conduct alleged. As such, X's tort claims do not arise out of, relate to, or depend upon the Terms or the existence of any contract. The forum selection clause, therefore, does not supply jurisdiction.

***B. X Has Not Plausibly Alleged Specific Personal Jurisdiction.***

Without a contractual waiver, X looks to minimum contacts for personal jurisdiction, alleging Bright Data "knowingly directed prohibited conduct to California and California residents" because X "has its principal place of business in California," Bright Data "offers its data sets and scraping tools for sale in California and to California residents," and "targeted [X's] users located in California." FAC ¶ 9. But to establish specific jurisdiction, X must show that Bright Data "expressly aimed [its conduct] at the forum state," and that those activities "caus[ed] harm that the defendant [knew was] likely to be suffered in the forum state." *Cont'l Appliances, Inc. v. Thomas*, 2012 WL 3646887, \*2 (N.D. Cal. 2012). X's allegations only concern X's connection to California or Bright Data's *lawful* conduct. That is not enough.<sup>7</sup>

<sup>7</sup> X does not and cannot assert general jurisdiction. Bright Data is an Israeli company. *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 924 (2011); *BNSF Ry. Co. v. Tyrrell*, 581 U.S. 402, 414 (2017) (no general jurisdiction where defendant had over 2,000 miles of railroad

1                   **1.       X Cannot Base Specific Jurisdiction on X's Own Domicile.**

2           X's "principal place of business" in California is irrelevant. FAC ¶ 9. "[I]t is the defendant,  
3 *not the plaintiff* ..., who must create contacts with the forum State." *Walden v. Fiore*, 571 U.S.  
4 277, 278, 290-91 (2014) ("mere injury to a forum resident is not [] sufficient" because the "focus"  
5 of the jurisdictional inquiry is on *where the "relevant conduct" took place*, not just the fact that  
6 the "conduct affected plaintiffs with connections to the forum State."); *Shopify*, 2023 WL 8225346,  
7 \*16 ("Does [Plaintiff's] ... California connection matter to the analysis of whether Shopify expressly  
8 aimed its activities toward California? *The answer is no*"). Nor can X make its domicile relevant  
9 by asserting that Bright Data "targeted" X. "[T]he mere fact [the alleged] conduct affected  
10 plaintiffs with connections to the forum State [does] not suffice to authorize jurisdiction." *Bristol-*  
11 *Myers Squibb Co. v. Superior Court*, 582 U.S. 255, 265 (2017). Following *Bristol-Myers*, courts  
12 have repeatedly held that "the case law does not support [the] position that a defendant's  
13 knowledge of a plaintiff's residence in the forum is enough" for specific jurisdiction. *E.g., Cont'l*  
14 *Appliances, Inc.*, 2012 WL 3646887, \*3. A defendant does not expressly aim its conduct toward  
15 California "simply because [it] allegedly directed [its] conduct at plaintiffs whom [it] knew had  
16 [California] connections." *Shopify*, 2023 WL 8225346, \*8.

17                   **2.       X Cannot Base Specific Jurisdiction on the Alleged Existence of**  
18                   ***Bright Data's Sales Office or the Location of Certain Employees.***

19           Allegations of Bright Data's California "sales office" and employees similarly do not  
20 establish specific jurisdiction. FAC ¶¶ 10-12, 15. Even if true, such contacts only establish a  
21 lawful presence in the forum; they do not "cause" plaintiffs' injury or give rise to X's claim.

22           *Shopify* controls. There, the Ninth Circuit first "narrow[ed] [the] allegations to the conduct  
23 relevant to the specific jurisdiction inquiry." *Shopify*, 2023 WL 8225346, \*5. Allegations that  
24 Shopify "does extensive business in the state," has "contracts with California merchants," has a  
25 "Los Angeles 'store' that promotes merchant relations," operates a "California fulfillment center,"  
26 has a "partnership with Stripe (a California company)," and has a subsidiary with a large "presence

27 \_\_\_\_\_  
28 track and 2,000 employees in Montana, because the inquiry is whether it is "at home" in the forum,  
not the "magnitude of the defendant's in-state contacts").

1 in the state (including business registration, employees, etc.)” were all irrelevant, because there is  
 2 “no causal relationship between Shopify’s broader California business contacts and [plaintiff’s]  
 3 claims because [those] those “contacts did not cause [plaintiffs’] harm.” *Id.*

4 In reaching this conclusion, the Ninth Circuit required strict proximate causation: a  
 5 “**strong, direct connection** between the defendant’s forum-related activities and the plaintiff’s  
 6 claims,” not just but for causation. *Id.* at \*6. “To the extent [plaintiff] suggests that [defendant’s]  
 7 broader business actions in California set the wheels in motion for [the defendant] to eventually  
 8 inflict ... harm on him in California, such **a butterfly effect theory of specific jurisdiction would**  
 9 **be far too expansive to satisfy due process.**” *Id.* As such, only acts that **directly** give rise to  
 10 plaintiff’s claims can be considered. Allegations of offices and employees do not qualify.

### 11 3. ***X Cannot Base Specific Jurisdiction on Bright Data’s Sale of General- 12 Purpose Scraping Services.***

13 Nor can X fill the jurisdictional void by alleging that Bright Data is a global internet  
 14 company that “offers its data sets and scraping tools for sale in California and to California  
 15 residents” and elsewhere. FAC ¶ 9. These services are not unlawful, so offering them in  
 16 California, or even “specifically target[ing] the California market” does not constitute *tortious*  
 17 *conduct* in or aimed at California.

18 *Shopify* again resolves the question. Addressing a question of “first impression,” the court  
 19 held that “[w]hen a company operates a **nationally available e-commerce payment platform** and  
 20 is indifferent to the location of end-users, the extraction and retention of consumer data, without  
 21 more, does not subject the defendant to specific jurisdiction in the forum where the online purchase  
 22 was made.” *Shopify*, 2023 WL 8225346, \*1. Shopify contracted with merchants in California  
 23 and elsewhere to operate the merchants’ ecommerce platform. In doing so, Shopify allegedly  
 24 violated California consumers’ privacy rights when California purchasers used Shopify to buy  
 25 products from California merchants. But there was no specific jurisdiction because Shopify  
 26 operated a nationwide platform. Web platforms cannot be “subject[] ... to [personal] jurisdiction  
 27 ... in every forum in which the website” was “accessible.” *Id.* at \*8. Ruling otherwise, the court  
 28 held, would impinge on defendants’ due process rights and would “lead to the eventual demise of

1 all restrictions on personal jurisdiction.” *Id.* at\*12.

2 Here, Bright Data is an Israeli internet service provider operating a *global* proxy network  
 3 and associated web scraping (and other) tools. While it certainly has some California customers  
 4 – as did Shopify – that does not mean it “expressly aimed” its conduct at California. “[A]  
 5 defendant foreseeably profiting from persons making online purchases in California does not  
 6 demonstrate express aiming.” *Id.* at \*13. Nor does X’s allegation that Bright Data advertised its  
 7 offerings in California suffice, *see* FAC ¶ 13, because “the use of geo-located advertisements  
 8 [does] not constitute express aiming when users in every forum ... would receive ads targeted to  
 9 their locations.” *Shopify*, 2023 WL 8225346, \*10. Similarly, X’s allegation that Bright Data offers  
 10 – as part of its proxy network – California IP addresses *for use by third-parties* does not suffice.  
 11 Bright Data offers IP addresses in virtually every jurisdiction that any user of its service can  
 12 choose. The “[a]ctions of [those] third parties” are not “reflective” of Bright Data’s express  
 13 aiming, but instead are the unilateral acts of third-parties. *Id.* at \*11. There is no difference  
 14 between Bright Data offering California IP addresses and Shopify contracting with California  
 15 merchants to offer ecommerce services. If it was not enough in *Shopify*, it is not enough here.

16 Indeed, this is an easier case than *Shopify*. In *Shopify*, there was no question that the  
 17 plaintiffs’ cause of action arose out of – and was directly tied to – conduct in California (Shopify’s  
 18 alleged unlawful collection of California information from California consumers transacting with  
 19 California merchants). Here, in contrast, X has not alleged any *unlawful* act in California. To see  
 20 this, it is necessary to assess the elements of each alleged tort. *See Schentag v. Nebgen*, 2018 WL  
 21 3104092, \*16 (S.D.N.Y. 2018) (the “analysis necessarily includes consideration of the claims’  
 22 elements and where the conduct occurred”); *Carroll v. J.M. Smucker Co.*, 2023 WL 4053796, \*3  
 23 (N.D. Cal. 2023) (Alsup, J.) (“The exact form of our [express aiming] analysis ... depends, to a  
 24 significant degree, on the specific type of tort or other wrongful conduct at issue.”).<sup>8</sup>

25  
 26 <sup>8</sup> *See also Bristol-Myers*, 582 U.S. at 264 (rejecting “sliding scale” weighing of contacts unrelated  
 27 to the claim)’ *Hanson v. Denckla*, 357 U.S. 235, 250-53 (1958) (the “*cause of action*” must “arise[]  
 28 out of” the defendant’s forum contacts); *Matus v. Premium Nutraceuticals, LLC*, 715 F. App’x  
 662, 662-63 (9th Cir. 2018) (without “*suit-related*” conduct ... creat[ing] a substantial connection  
 with the forum ..., specific jurisdiction is lacking regardless of the extent of a defendant’s

1        ***Tortious Interference.*** There is no allegation that Bright Data ***induced*** a California  
 2 customer to breach X’s Terms. X only alleges that Bright Data “marketed and sold its scraping  
 3 tools to X users and account holders” in California. FAC ¶¶ 9, 74-75. ***But scraping is not illegal.***  
 4 So, the sale of lawful scraping services is not unlawful inducement. And if the sale of general  
 5 scraping services is not unlawful inducement, then the sale of those services to California residents  
 6 is also not tortious conduct in or aimed at California. X must allege something more. But X does  
 7 not, for example, say that Bright Data told X’s California users that they should use their accounts  
 8 to scrape X sites *behind* a log-on screen. There is no allegation that Bright Data’s services  
 9 distinguish between third-parties that have contracts with X and members of the general public  
 10 that do not. Instead, X alleges that Bright Data was “aware” its services ***might*** be used for  
 11 unauthorized scraping. See FAC ¶ 73. But an internet service provider offering a lawful service  
 12 globally is not, by that fact alone, subject to tortious interference claims in every jurisdiction where  
 13 a third-party might improperly use its services.

14        This principle flows directly from this Court’s decision in *Smith v. Facebook, Inc.*, 262 F.  
 15 Supp. 3d 943 (N.D. Cal. 2017). There, the plaintiffs alleged that non-resident healthcare  
 16 companies improperly sent sensitive medical information to Facebook, which used the information  
 17 to target unsuspecting users with unwanted advertising. The court found that, though Facebook’s  
 18 “tracking” was continuous and systematic, and occurred in California, the non-resident healthcare  
 19 defendants did not “direct[] their activities” at California “even if [they] knew” that their actions  
 20 allowed Facebook to track users from California. *Id.* at 951-52. As the Court explained:

21        “Embedded third-party code is ubiquitous, not just in the form of Facebook buttons,  
 22 but also in the form of videos, ads, analytics services, code libraries, content  
 23 delivery networks, and myriad other tools. Under Plaintiffs’ theory, every website  
 24 operator that embeds one of these tools could be haled into court where the third-  
 25 party company resides. Personal jurisdiction cannot reasonably stretch so far.” *Id.*

26        The same principle applies here. If merely offering a lawful service globally subjects an  
 27 internet service provider to jurisdiction based on a third-party’s alleged improper forum-conduct,

28        *unconnected activities in the State*”); *Picot v. Weston*, 780 F.3d 1206, 1211 (9th Cir. 2015) (“the  
***claim*** must be one which arises out of or relates to the defendant’s forum-related activities”).



1 then every internet service provider – including X – would be subject to personal jurisdiction  
 2 wherever it has a customer. That is not the law. *Adobe Sys. Inc. v. Nwubah*, 2019 WL 6611096,  
 3 \*1 (N.D. Cal. 2019) (online sale of goods nationally, including to consumers in California, did not  
 4 “expressly aim” its conduct at California); *ICC LLC v. WhatsApp Inc.*, 2013 WL 5230631, \*4  
 5 (E.D. Va. 2013) (rejecting argument that “every district in the United States has jurisdiction over  
 6 WhatsApp because it has 300 million users”).

7 ***X’s Other Tort Claims.*** X also fails to allege that any California-directed conduct gave  
 8 rise to any of X’s unjust enrichment, trespass, misappropriation, and UCL claims. The gravamen  
 9 of each of these claims is that X operates servers (where, has not been alleged), and that Bright  
 10 Data (or its customers) accessed them. But X has not alleged that all its servers are located in  
 11 California, or that Bright Data knows where they are. If for example, X operates servers in  
 12 Virginia, Utah, or Ireland, then searches touching those servers would not involve any California  
 13 contacts. Nor would Bright Data’s directing a request to X’s website constitute purposeful  
 14 direction anywhere if Bright Data has no idea where X’s servers are located (or to which X server  
 15 its request might be directed). The happenstance of where X might have a server cannot create  
 16 jurisdiction, because plaintiffs’ contacts with the forum are irrelevant. *See Shopify*, 2023 WL  
 17 8225346, \*7 (where “injury is entirely personal to [plaintiff] and would follow him wherever he  
 18 might choose to live or travel,” “[t]he effects of [the defendant’s] actions are therefore ‘not  
 19 connected to the forum State in a way that makes those effects a proper basis for jurisdiction.’”).<sup>9</sup>  
 20  
 21

---

22 <sup>9</sup> See also, e.g., *Man-D-Tec, Inc. v. Nylube Prods. Co., LLC*, 2012 WL 1831521, \*2 (D. Ariz. 2012)  
 23 (“If the mere location of a server could create personal jurisdiction, any state where a server is  
 24 located would have personal jurisdiction over any user of that server”); *Doe v. Geller*, 533 F. Supp.  
 25 2d 996, 1009 (N.D. Cal. 2008) (“If plaintiff’s theory of jurisdiction were upheld, then the Northern  
 26 District of California could assert jurisdiction over every single takedown notice ever sent to  
 27 YouTube or any other company in Silicon Valley”); *Chang v. Virgin Mobile USA, LLC*, 2009 WL  
 28 111570, \*3 (N.D. Tex. 2009) (Plaintiffs “cannot rely on the fortuitous location of Flickr’s servers  
 to establish personal jurisdiction over Virgin Australia”) (citing *Ray v. Experian*, 2007 WL  
 4245459, \*3 (N.D. Tex. 2007) (holding that defendant’s “accessing or sending data ... to or from  
 a database which happens to be headquartered in Texas is not purposeful availment by [defendant]  
 of the benefits and protections of Texas’ laws”).

1                   4.       ***The Conclusory Allegation that Bright Data “Targeted” X’s California***  
2                   ***Users Does Not Establish Specific Jurisdiction.***

3                   In its final jurisdictional salvo, X says that specific jurisdiction exists because Bright Data  
4                   “target[ed] ... X Corp.’s users located in California.” FAC ¶¶ 9, 13. As an initial matter, even if  
5                   this sufficed to establish jurisdiction, X’s claims for scraping by *non-California* users would need  
6                   to be dismissed. Put simply, even under X’s argument, any tortious interference claim based on  
7                   scraping by third-parties located in India, China, Timbuktu – or even Las Vegas – cannot be  
8                   brought in this Court. *See Bristol-Myers*, 582 U.S. at 264-68 (requiring claim-by-claim analysis,  
9                   and finding jurisdiction for California residents’ claims, but not non-residents’ claims).

10                  But even as to X’s California users, X’s conclusory allegation of “targeting” does not  
11                  satisfy its pleading burden. *Swartz v. KPMG LLP*, 476 F.3d 756, 766 (9th Cir. 2007) (“bare bones  
12                  assertions of minimum contacts ... unsupported by specific factual allegations will not satisfy a  
13                  plaintiff’s pleading burden”). Otherwise, a plaintiff could create jurisdiction simply by inserting  
14                  the word “targeting” in front of otherwise deficient factual allegations. The word “targeting” is  
15                  not only a legal conclusion and conclusory label, it is also inherently vague. What did Bright Data  
16                  do to “target” California users? X does not say. To the extent X simply means that Bright Data  
17                  sold its scraping services to California customers with an X account (FAC ¶ 14), the allegation  
18                  fails for the reasons discussed: Selling a lawful service to customers that happen to have an X  
19                  account is not unlawful inducement, even if the customer misuses the service.

20                  X gets no further by alleging that Bright Data “used [its] X accounts to discuss and promote  
21                  their data-scraping products and services.” FAC ¶ 45. Bright Data’s mere use of an X account to  
22                  advertise its services does not establish that its *content* constitutes tortious inducement (X does not  
23                  allege it does) or was directed to *California* users (X does not allege it was). Indeed, none of these  
24                  advertisements or posts even mention Twitter. Rather, they speak generically about Bright Data’s  
25                  scraping tools and services. If the sale of those services does not constitute “inducement,” then  
26                  neither does advertising those services.<sup>10</sup>

27  
28                  <sup>10</sup> For the same reason, X’s allegation that Bright Data operates an “interactive website,” *see* FAC  
                ¶ 81, does not establish *tortious conduct* aimed at California. *Shopify*, 2023 WL 8225346, \*8



Nor can X establish personal jurisdiction by pointing to Bright Data’s webpage explaining how Bright Data’s tools can be used to scrape public Twitter information. Just as Twitter posts are not directed to California, neither is Bright Data’s website. It is visible to anyone in the world. Nor is Bright Data’s website directed toward X *users*. It may explain that Bright Data’s services can be used to scrape public Twitter data, but that does not require a Twitter account. So Bright Data’s public statements do not establish unlawful inducement of a third-party breach, let alone inducement directed to California. *Carroll*, 2023 WL 4053796, \*3 (no jurisdiction where the “interactive features” of a website were not specifically targeted to California).

#### IV. X FAILS TO STATE A CLAIM FOR TORTIOUS INTERFERENCE.

Even if the Court has jurisdiction, X fails to state a claim for tortious interference. “To state a claim ..., [X] must allege: (1) a valid contract between plaintiff and a third party; (2) defendant’s knowledge of this contract; (3) defendant’s intentional acts designed to induce breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damages.” *Mishiyev v. Alphabet, Inc.*, 444 F. Supp. 3d 1154, 1160-61 (N.D. Cal. 2020) (Alsup, J.). Here, X has not properly pled an underlying breach of its third-party contracts, or that Bright Data knew of, or induced a breach of, them.

##### A. X Fails to Allege Breach of any Valid and Enforceable Third-Party Contract.

While X might be popular, it does not contract with everyone. To allege “defendant’s knowledge” of “a valid [contract] between the plaintiff and a third party,” X must “stat[e] which third parties, if any, Plaintiff had a contract with.” *Soil Retention Prods., Inc. v. Brentwood Indus., Inc.*, 521 F. Supp. 3d 929, 960-61 (S.D. Cal. 2021). X never did.

X does not identify a *single* person that engaged in any prohibited scraping activity. Instead, it speculates there may be some unknown cadre of shared customers using “automated means” to search X’s site and scrape data. FAC ¶¶ 82, 84. That does not plead a breach of an underlying contract between X and any third-party scraper. *Mishiyev*, 444 F. Supp. 3d at 1160-61 (dismissing tortious interference claim where plaintiff “fail[ed] to identify any contract between  
\_\_\_\_\_  
 (“operation of an interactive website does not, by itself, establish express aiming.”).

1 himself and a third party,” but merely alleged that he had “many subscribers”); *In re Charles*  
 2 *Schwab Corp. Sec. Litig.*, 257 F.R.D. 534, 552 (N.D. Cal. 2009) (Alsup, J.) (dismissing claim  
 3 where “the complaint never identifies the parties to the alleged contract”); *Soil Retention Prods.,*  
 4 *Inc.*, 521 F. Supp. 3d at 959-60 (dismissing claim where complaint “presupposes that Defendant  
 5 knew of Plaintiff’s contracts with third parties and intended to disrupt those contracts”).<sup>11</sup>

6 Contrast this with X’s breach of contract claim, where it at least alleges that Bright Data  
 7 had an account and scrapes X. These are necessary allegations. Imagine if X omitted allegations  
 8 concerning contract formation; or that X alleged Bright Data has a contract but failed to allege the  
 9 breach. Either would be fatal to the claim. Here, because a breach of a third-party contract is a  
 10 predicate for any tortious interference claim, X must allege the breach with the same specificity as  
 11 its breach of contract allegations against Bright Data. It has not.

12 Even putting identities aside, X does not allege a valid contract between X and any third-  
 13 party scraper. At most, X alleges that customers “who purchased Defendant’s scraping services  
 14 and tools used them ... to scrape data from the X platform.” FAC ¶ 84. But that does not establish  
 15 a valid contract because it does not show that the third-party had *agreed* to the Terms.

16 There are two main types of internet-based contracts: clickwrap and browser-wrap. *See*  
 17 *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1175-76 (9th Cir. 2014) (distinguishing between  
 18 them). Clickwrap contracts arise when a user creates an “account” and clicks “I agree.” Browser-  
 19 wrap, in contrast, does not involve express acceptance. Rather, in *limited* circumstances, courts  
 20 may imply acceptance based on the parties’ conduct. Here, X has not alleged facts demonstrating  
 21 that any third-party scraper is bound by a clickwrap or browser-wrap.

22 As to clickwrap, X does not allege that any third-party scraper had an X account. Users of  
 23 Bright Data’s “tools and services” do not need an X account to access X’s public website. Anyone  
 24 with a browser can do that. So, the mere fact a third-party uses Bright Data’s services to access X

---

25  
 26 <sup>11</sup> *See also UMG Recordings, Inc. v. Glob. Eagle Ent., Inc.*, 117 F. Supp. 3d 1092, 1115 (C.D. Cal.  
 27 2015) (plaintiff “must **identify** the third party”); *Green Crush LLC v. Paradise Splash I, Inc.*, 2018  
 28 WL 4940825, \*9 (C.D. Cal. 2018) (dismissing complaint that “failed to plead the identity” of the  
 third-party); *San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1094 (N.D. Cal. 2018) (“plaintiff must  
 allege a relationship with ‘a **specific**, albeit unnamed’ third party.”).

1 does not supplant the need to allege an X account. And without an account, there is no clickwrap.

2 Absent clickwrap, X tries its hand at browser-wrap, saying that anyone who visits an X  
3 website *implicitly* agrees to “abide by the Terms.” FAC ¶ 79. But website visitation does not  
4 establish a valid and enforceable browser-wrap agreement. This is so for two reasons. *First*, X  
5 does not allege that any of these unidentified third-party scrapers had notice of the Terms. *See*,  
6 *e.g.*, *Olney v. Job.com, Inc.*, 2014 WL 4660851, \*\*4-6 (E.D. Cal. 2014) (“Job’s allegation that its  
7 website contained a hyperlink to the terms is insufficient to demonstrate that TPDs were put on  
8 notice of the term’s existence or that TPDs assented to them by virtue of their use of the website  
9 alone.”). At most, X alleges that “*Defendant* is aware of the Terms and that they govern all users  
10 who choose to interact with the X platform.” FAC ¶ 73. But contract formation between X and a  
11 *third-party* depends – not on Bright Data’s awareness – but on the third-party’s.<sup>12</sup>

12 *Second*, any alleged browser-wrap contract fails for *lack of consideration* because X has  
13 no legal right to prevent *anyone* from searching the public web. To provide consideration, X must  
14 offer its users something that they are not already entitled to. But Bright Data’s scraping tools  
15 only permit customers to search *public* information. *See* FAC ¶ 45(c) (“*public* web data.”); ¶ 56  
16 (“*public data*”). This is information that, even according to X’s Terms, is owned by individual  
17 *users*, *not X*. *See* Ex. 1 § 3 (“You retain your rights to any Content you submit, post or display on  
18 or through the Services. What’s yours is yours — *you own your Content*.”). Nor does X assert  
19 any *copyright* or other *property* interest that prevents public search. Because X lacks any legal  
20 right to block any third-party from scraping information that X has chosen to make publicly  
21

---

22 <sup>12</sup> Similarly, the conclusory allegation that Bright Data was “aware” that the Terms “govern all  
23 users who interact with the X platform,” even if true (it isn’t), is not the same as Bright Data’s  
24 awareness that each customer was aware of the Terms. That is, a tortious interference claim based  
25 on a *browser-wrap* claim requires two levels of knowledge: the underlying scraper’s knowledge  
26 of the Terms sufficient to bind the third-party scraper, and Bright Data’s knowledge that the third-  
27 party possessed such awareness. *See Orchard Supply Hardware LLC v. Home Depot USA, Inc.*,  
28 967 F. Supp. 2d 1347, 1364-65 (N.D. Cal. 2013) (dismissing claim, even after repleading to allege  
specific customers subject to plaintiff’s “Universal Terms and Conditions,” because plaintiff still  
“failed to allege that [the defendant] knew of the relevant contracts, which is a required element in  
the claim”). X alleges neither. Instead, it simply alleges that Bright Data was aware of X’s *legal*  
*position* that any person who has visited X is contractually bound. That is not enough.

1 available, it has not provided any consideration to third-parties when they exercise their right to  
2 search the web. Without consideration, there is no contract and no tortious interference.

3 ***B. Offering a Lawful Service is Not Inducement.***

4 Even if X had properly alleged the existence of a valid underlying third-party contract, it  
5 has not alleged a knowing inducement of a breach. This is not a case where the defendant's  
6 services can only be used for illicit purposes. *Cf. Blizzard Ent. Inc. v. Ceiling Fan Software LLC*,  
7 28 F. Supp. 3d 1006, 1011-12, 1016 (C.D. Cal. 2013) (involving "single-purpose software products  
8 ... designed to operate only" with plaintiffs' video game and for "no other purpose than to engage  
9 in game play that is expressly prohibited by the EULA and ToU"); *Ticketmaster L.L.C. v. RMG*  
10 *Techs.*, 2007 WL 2989504, \*3 (C.D. Cal. 2007) ("The FAC alleges that Defendant made a false  
11 promise ... each time it used the website.").

12 Because Bright Data's services have countless legitimate purposes, X must allege that  
13 Bright Data knew that its customers were "certain or substantially certain" to use the services for  
14 illicit purposes. Rest. 2d Torts § 766, cmt. j; *id.* § 8A ("The word 'intent' ... denote[s] that the  
15 actor desires to cause consequences of his act, or that he believes that the consequences are  
16 substantially certain to result from it."); *Nevada DeAnza Fam. Ltd. P'ship v. Tesoro Re. & Mktg.*  
17 *LLC*, 474 F. Supp. 3d 1087, 1095 (N.D. Cal. 2020) (dismissing claim where "complaint does not  
18 allege [the defendant] knew with substantial certainty that its actions would interfere with the  
19 [plaintiff's contract]"); *Sebastian Int'l, Inc. v. Russolillo*, 162 F. Supp. 2d 1198, 1205 (C.D. Cal.)  
20 ("Plaintiffs must show that [defendants] knew with at least substantial certainty that a necessary  
21 consequence of their actions" would be interference).

22 Consider a simple hypothetical. It's 1968. An electronics manufacturer sells a dual-sided  
23 cassette deck that can copy music from one tape to another. If a consumer uses it for personal  
24 reasons, it is perfectly lawful. If the consumer makes production copies and sells them out of the  
25 back of his car, it isn't. Because the manufacturer neither intended the device to be used  
26 improperly nor could be "substantially certain" that any particular customer would do so, there is  
27 no liability, even if the manufacturer knows that it is likely that someone will misuse it.

On that score, the Supreme Court’s recent decision in *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023), controls. There, plaintiffs sued Twitter “for allegedly aiding and abetting ISIS,” claiming that ISIS “used defendants’ social-media platforms to recruit new terrorists and to raise funds for terrorism,” and that Twitter “*knew* that ISIS was using their platforms but failed to stop it from doing so.” *Id.* at 478. The Supreme Court affirmed dismissal under Rule 12(b)(6). Expressing concern that “ordinary merchants could become liable for any misuse of their goods and services” by third parties, the Court explained that “the concept of ‘helping’ in the commission of a ... tort ... has never been boundless.” *Id.* at 488-89. As such, internet service providers do not become secondarily liable simply because their services are misused. As the Court held:

**“The mere creation of those platforms ... is not culpable.** To be sure, it might be that bad actors like ISIS are able to use platforms like defendants’ for illegal – and sometimes terrible – ends. But the same could be said of cell phones, email, or the internet generally. Yet, we generally do not think that internet or cell service providers incur culpability merely for providing their services to the public writ large.... The fact that some bad actors took advantage of these platforms is insufficient to state a claim that defendants knowingly gave substantial assistance and thereby aided and abetted those wrongdoers’ acts.... [A] contrary holding would effectively hold any sort of communication provider liable for any sort of wrongdoing *merely for knowing* that the wrongdoers were using its services and failing to stop them. **That conclusion would run roughshod over the typical limits on tort liability.**” *Id.* at 499, 503.

Here, X does not allege Bright Data was “substantially certain” its customers would use its services for illicit purposes. X only points to general purpose tools, such as Bright Data’s proxy services and tools, that can be used for countless legitimate purposes, including accessing non-X sites. *See* FAC ¶ 82. Considering the many legitimate uses for Bright Data’s services, the mere allegation that Bright Data sold scraping services does not satisfy X’s burden of pleading “substantial assistance” for a specific “actionable wrong.” *Taamneh*, 598 U.S. at 495. For that reason, its speculation – that there may be some shared customers that use Bright Data’s services for improper purposes – does not constitute a plausible allegation of unlawful *inducement*.

#### V. X FAILS TO STATE A CLAIM FOR UNJUST ENRICHMENT.

X’s unjust enrichment claim fails because X does not have an independent property right to prevent Bright Data from searching the public web. “California does not recognize a stand-

alone cause of action for unjust enrichment.” *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031 (N.D. Cal. 2012). So, courts “construe [an unjust enrichment] cause of action as a quasi-contract claim seeking restitution.” *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015); *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016) (same). Here, “the only possible premise of [X’s] cause of action of unjust enrichment is that [it] is entitled to restitution ... on a quasi-contract or assumpsit theory.” *McBride v. Boughton*, 123 Cal. App. 4th 379, 387-89 (2004).

Implied-in-law quasi-contracts fall under Section 69(2) of the Restatement. “An offeree who does any act inconsistent with the *offeror’s ownership of offered property* is bound in accordance with the offered terms unless they are manifestly unreasonable.” Restatement (Second) of Contracts § 69(2). This is the modern equivalent of waiving the tort and suing in assumpsit, which applies to situations like shoplifting, theft, and misappropriation of property. *See id.* § 4 cmt. b. To state a claim, X must show that (i) it “owns” the public data Bright Data searches, or that it has a non-contractual right to restrict access to it; (ii) Bright Data’s public search constitutes an act “inconsistent with” X’s ownership; and (iii) it would not be unreasonable to enforce X’s browser-wrap restraints. *Id.* § 69(2). X has not alleged any element.

***X Does Not Own the Internet.*** X cannot use quasi-contract to block public web search, because X does not own the Internet. It is literally that simple. X and its users have made certain information publicly available. Having chosen to make the information public, X cannot claim any independent property interest. With no independent property right to prevent scraping, X cannot rely on quasi-contract or unjust enrichment to remedy a breach of that non-existent right.<sup>13</sup>

---

<sup>13</sup> Even if the Court ultimately concludes that X has an enforceable property right, any claim for “unjust enrichment” prior to the Court’s declaration that such a property right exists fails, since a quasi-contractual unjust enrichment claim presupposes an *undisputed* property right. Rest. 2d Contracts § 69, cmt. e, illus. 10 (“Under a claim of right made in error but in good faith, A digs a well on B’s unused land and takes water therefrom... B notifies A that he will charge A \$50 a day for every day on which A takes water from his land. Even after it is adjudicated that A’s right is nonexistent, ***A does not accept B’s terms by taking water.***”). A simple example illustrates. Suppose a copyright owner tells a teacher, if you cite my article, you owe me \$100, and the teacher says in good faith, “fair use, I owe you nothing.” Copyright may provide a cause of action, but quasi-contract will not enforce the terms of this fictional (non) meeting of the minds. Here, Bright Data has a reasonable and good faith belief that X has no ***non-contractual*** property right to block



***Bright Data Has Not Acted Inconsistently with X's (Unalleged) Ownership Interest.***

Even if X could identify an ownership interest, Bright Data does not engage in an “act inconsistent” with that interest when it searches the web. Internet access presupposes the ability to search public websites. It does not make web surfers beholden to those who publicly post information. If Taylor Swift posts information about her upcoming concerts on her public X page, she has not formed a quasi-contractual relationship with each of the millions of fans who view that page. Nor has X entered into a quasi-contractual relationship with those same fans when they view the web page. Everyday experience confirms this. Consider the following:

- A person browses a law firm’s website to check his adversary’s bio. He is not using the law firm’s services; he is *viewing* the law firm’s advertising materials.
- A person walks down the street and stops to browse a menu posted on an outside window. He is not using the restaurant’s services; he is *viewing* its advertising.
- A person clicks on a Google link and is redirected to the New York Times public Instagram page. That page contains teaser information about the New York Times Cooking section along with a sign-in request to get more information about featured recipes. That person is not using Instagram’s or the New York Times’s services; he is *viewing* the New York Times’s Instagram advertising.

The Internet is a “social contract.” Anyone can connect their servers to the Internet to make their websites available to the public, and anyone else can use their browsers to search those websites. When they do, neither has become quasi-contractually bound to the other. They are each simply exercising their God-given freedom.

Nor can X deprive Bright Data of this freedom by asserting that (i) Bright Data “[has] used X Corp.’s service, platform, and computer network without authorization to scrape data from the X platform” and (ii) Bright Data has “receive[d] benefits” from doing so. FAC ¶¶ 89, 90. Nothing compelled X to connect its servers to the internet or make information freely available without a login or password. It chose to do so, presumably to attract enough “eyeballs” to make its platform attractive to tweeters and advertisers. When a street fair vendor displays artwork for all to see and enjoy, any person is free to walk up to the stall and take a gander. The vendor has no right to say:

---

Bright Data from searching the public web. An unjust enrichment claim, therefore, does not lie.

1 “It’s mine, you must close your eyes or I’ll sue.” Of course, the vendor still holds title to the  
2 artwork, and if it is taken, the vendor can sue for conversion. But here, X does not bring a  
3 conversion claim because Bright Data did not take any property owned by X.

4 Nor does it matter that Bright Data allegedly “receive[d] benefits” from searching the  
5 public web. The “mere fact that a person benefits another is not of itself sufficient to require the  
6 other to make restitution therefor.” Restatement (First) of Restitution § 1, cmt. c. “[O]ne who  
7 improves his own land ordinarily benefits his neighbors to some extent,” but as the Restatement  
8 illustrates, he is not “entitled to restitution.” *Id.* Just like a homeowner who plants colorful flowers  
9 in her front yard, X put information into the public domain. Neither has a claim for restitution  
10 when Bright Data or a passerby takes a gander.

11 ***Blocking Public Web Search Absent a Valid Contract is Against Public Interest.*** X’s  
12 quasi-contract or unjust enrichment claim also fails because blocking public search unreasonably  
13 restrains trade. As the Restatement makes clear, unreasonable quasi-contractual restraints are  
14 unenforceable. *See* Rest. 2d Contracts §§ 69(2), 187. A restraint is “necessarily unreasonable”  
15 unless it is “subsidiary to an otherwise valid transaction or relationship.” *Id.* at § 187 & cmt. b.  
16 But as noted above, an unjust enrichment claim presupposes the absence of a valid transaction or  
17 relationship (since such a relationship would be governed by contract law). Without a valid and  
18 enforceable contractual relationship, any restraint on automated scraping – by definition – cannot  
19 be ancillary. So if X is proceeding *quasi-contractually*, it cannot enforce *restraints* on Bright  
20 Data’s right to search the public web.

## 21 **VI. X FAILS TO STATE A CLAIM FOR TRESPASS TO CHATTELS.**

22 The common law doctrine of “trespass to chattels” does not give X the dictatorial right to  
23 pick and choose who may surf the web. When a person surfs the web, she is exercising her right  
24 to surf the web; she is not trespassing on website operators who have voluntarily hooked up their  
25 servers to the Internet. A simple analogy makes the point: You call up Verizon and install a phone  
26 line. Do you now have a trespass claim against any person who dials your number? Clearly not.  
27 Like the telephone before it, the Internet is a free and open communications network. When  
28



participants' servers communicate with each other by sending and receiving encoded electrons, neither is trespassing on the other's property. Here, Bright Data's servers requested public information from X's servers, and X's servers voluntarily delivered that information in accordance with standard internet protocols. That is not a trespass.

**A. Public Internet Search Does Not Constitute a Trespass.**

A trespass involves interference with the personal property of another without consent. Consent *negates* any trespass claim. See Rest. 2d Torts, §§ 49, 50; *Price v. Apple, Inc.*, 2022 WL 1032462, \*6 (N.D. Cal. 2022) ("consent dooms [a] trespass claim). Consent can be "manifested by action or inaction," and "need not be communicated" to the alleged trespasser. Rest. 2d Torts § 892(1).

Here, X consented to participate in a worldwide communications network, known as the World Wide Web, when it connected its servers to the Internet. The second it did, it joined hundreds of millions of people who also enjoy the right (and obligation) to send and receive communications through the network, according to standard Internet Protocols. No separate consent was necessary to allow web surfers to contact X's servers, because when a person participates in a group endeavor, that person consents to any contact normally associated with it. *Id.*, § 50, cmt. b ("Taking part in a game manifests a willingness to submit to such bodily contacts or restrictions of liberty as are permitted by its rules or usages."); *id.* § 53, cmt. a (same).<sup>14</sup>

Nor can X claim that its consent was limited by the Terms posted on its website. Even where all participants *agree* that conduct is forbidden, such restrictions do not negate, obviate, or even limit consent unless the conduct is "totally outside the range of the ordinary activity involved" in the group activity. *Knight v. Jewett*, 3 Cal. 4th 296, 318 (1992). Baseball players *agree* not to

---

<sup>14</sup> See Eric J. Feigin, *Architecture of Consent: Internet Protocols and Their Legal Implication*, 56 Stan. L. Rev. 901, 931 (2004) ("While one might assert that an unwanted HTTP request is a real property trespass, in that one person caused a 'thing' (electronic impulses) to enter another person's property (their machine), this doesn't make sense [because] a bilateral contract was reached in which the server agreed to listen to what the client had to say. This is similar to my picking up the telephone to find that there's a solicitor on the other end .... I hardly have a cause of action for real property trespass if the solicitor starts to talk. If the server didn't want the request, it shouldn't have made the TCP contract.")

1 throw [a] beanball in retaliation” for perceived slights; basketball players agree not to foul other  
2 players; boxers agree not to punch below the belt. Though conduct may be “forbidden by the rules  
3 of the game,” it is not tortious because consent remains effective. By “enter[ing] the sport,” the  
4 player has “consent[ed] to physical contacts” within “the range of ordinary activity” associated  
5 with the endeavor, and other participants do not “exceed[] the scope of consent” just because the  
6 contact constitutes a rules violation. *See Hunt v. Zuffa, LLC*, 361 F. Supp. 3d 992, 1009 (D. Nev.  
7 2019) (no liability for physical injuries enhanced by illegal steroid use); *Avila v. Citrus Cmty. Coll.*  
8 *Dist.*, 38 Cal. 4th 148, 152 (Cal. 2006) (no liability for baseball “beanballs”); Rest. 2d Torts § 50,  
9 cmt. b (no liability for tackling an opponent while “offsides” in violation of the game rules).

10 Here, X does not allege that Bright Data violated the rules of Internet usage when it sent  
11 and received server communications. Instead, X argues that, even if Bright Data’s server requests  
12 were within the “range of ordinary” Internet usage, X can selectively limit consent to server  
13 requests that align with its business model. It cannot. If consent is not negated even when *all*  
14 participants agree to rules prohibiting certain conduct – for example, when official rules that  
15 *everyone agrees to* expressly bans intentional beanballs – then consent also isn’t limited when an  
16 individual player also says the same thing.

17 The standard is whether the contact is “totally outside the range” of ordinary activity  
18 associated with the endeavor. *Knight*, 3 Cal. 4<sup>th</sup> at 318. A football player, for example, is not the  
19 victim of a tort if he’s tackled while wearing a jersey that says, “don’t mess with me.” If he doesn’t  
20 like the rules, he can pick up his football and go home, but he can’t impose his own rules over the  
21 objections of the other participants who just want to play the game. The reason is simple. The  
22 jersey, in that example, is not the *source* of consent to participate in the group endeavor; the *act* of  
23 participating is. If the player wants to enjoy the benefits of playing the game, he has to consent to  
24 the contacts normally associated with it.

25 So too, because a website operator’s Terms are not the source of consent to participate in  
26 the Internet, they do not govern the metes and bounds of consensual server contact. Just imagine  
27 if X discriminatorily posted a sign that said anyone whose name begins with “A” can’t search X’s  
28

1 site. Would everyone from Alice to Alsup now be liable in trespass for typing in www.X.com into  
 2 their web browser? No. The Terms are merely a contractual offer that can be accepted or rejected.  
 3 If the Terms are accepted, then X might have a claim sounding in *contract*, but not tort. But if the  
 4 Terms are rejected – as Bright Data did here – they are null and void; they do not somehow survive  
 5 for the limited purpose of modifying consent.<sup>15</sup>

6 X’s argument to the contrary would create a dangerous precedent. It would mean that any  
 7 provision in its Terms can be enforced, not just by contract, but by tort. If a 12-year-old visits X’s  
 8 homepage, thereby violating X’s age restriction, has the child now become liable for punitive  
 9 damages for trespassing on X’s servers without consent? No, the law of trespass is not a  
 10 supercharged remedy for breach of X’s Terms. If X wants to withdraw its consent to receive  
 11 requests through the Internet, the way to do so is to unhook its servers from the Internet and create  
 12 a closed private network that only it and its invitees can use. It has not done so.

13 ***B. X Fails to Allege Intentional Interference with Its Property.***

14 X’s trespass claim also fails because it has not alleged intentional interference with X’s  
 15 property. In some cases, the manner in which a server request is made is so far removed from  
 16 normal internet usage that it exceeds the extent of implied consent, and can constitute a trespass if  
 17 it *significantly* and *intentionally* interferes with the website operator’s enjoyment of its property.  
 18 But here, Bright Data’s server requests are not so outside the normal and proper use of the Internet  
 19 that they negate consent. And even if they were, there has been no allegation of significant or  
 20 intentional interference. Put simply, *scraping is not illegal*. Google, the largest scraper on the  
 21 planet, for example, has not trespassed on every site included in its search results. Nor has Bright  
 22 Data trespassed when it scrapes those same sites for the same information.

23 Let’s return to the phone booth, and consider two scenarios. In the first, your phone rings,  
 24

---

25 <sup>15</sup> *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000), and its ilk, are  
 26 inapposite because they do not address whether the plaintiff consented by virtue of its participation  
 27 in a global communications network. In any event, the California Supreme Court sharply curtailed  
 28 *eBay* on interference grounds, holding that the tort “does not encompass ... an electronic  
 communication that [does not] impair[] [the system’s] functioning.” *See Intel Corp. v. Hamidi*, 30  
 Cal.4<sup>th</sup> 1342, 1347, 1357-60 (2003).

1 you pick it up, and are greeted with a recorded voice. You have just received a telemarketing call  
2 from a robocaller. The call may be unwanted, but there is no trespass because that is what phones  
3 are for: to send and receive information. That the call was “automated” or that the telemarketer  
4 made a similar call to every house in America is irrelevant. Because the purpose of the call was  
5 to communicate, the caller used the phone network for its intended purpose. Nor does it matter  
6 that the call was unwelcome, or even that the number was listed on the FTC’s “Do Not Call”  
7 registry. That may be a violation of FTC regulations, but it does not mean the telemarketer  
8 *intentionally* deprived the homeowner of the use of its landline, and it does not make the  
9 telemarketer liable according to the differing common laws of the several states.

10 In the second scenario, there is a dastardly prankster who makes thousands of calls to the  
11 same number, *not* for the purpose of communicating with the homeowner, but for the *purpose* of  
12 deliberately creating busy signals and depriving the homeowner of the use of the phone. The  
13 prankster’s use was not an intended or reasonable use of the nation’s telecommunications network.  
14 As such, the homeowner did not impliedly consent to those calls when it installed a phone line,  
15 and the prankster did not reasonably use the phone network when it *intended* to disrupt the  
16 homeowner from making and receiving calls from others. *See* Rest. 2d Torts, § 50, cmt. b (A  
17 football player that “deliberately injures” another player is liable in tort, regardless of the “rules  
18 and usages of football.”).

19 Here, X does not allege that Bright Data sent server requests for the purpose of interfering  
20 with X’s servers. Indeed, harming X’s servers would be antithetical to Bright Data’s mission as it  
21 would impair the availability of the information Bright Data was requesting. *See WhatsApp, Inc.*  
22 *v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 684-85 (N.D. Cal. 2020) (dismissing trespass claim  
23 where “defendants’ program was reliant on WhatsApp’s servers to function exactly as intended”).  
24 Here, Bright Data made server requests for purposes of requesting information from X’s servers,  
25 and X’s servers responded by providing the information requested. When a telemarketer calls  
26 your home and *makes a sale*, the homeowner who regrets the purchase and wishes he never picked  
27 up the phone cannot sue in trespass as the phone was used for its intended purpose. So too, when  
28

Bright Data makes a server request, and successfully receives the requested information, it used the Internet as the Internet was intended – a communications device. It has not trespassed.

**C. X Fails to Allege that Any Interference with Its Servers Has Been Substantial.**

Even if the Court finds that there has been some intentional interference, X’s trespass claim still fails because its conclusory allegations of harm do not suffice to establish a *substantial* interference with X’s use or enjoyment of its servers. *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1357 (2003); *Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp 3d 1056, 1080 (N.D. Cal. 2018); *Volkswagen Grp. of Am., Inc. v. Smartcar, Inc.*, 2022 WL 20184651, \*8 (N.D. Cal. 2022) (dismissing claim because “in the computer context, a defendant temporarily us[ing] some portion of [a company’s] computers’ processors or storage is ... not enough, there must be some measurable loss from the use of [the] computer system.”).

The gravamen of X’s complaint is that Bright Data scraped data from X’s site. That is not a *trespass* injury because information is not a *tangible* chattel. “Plaintiff’s interest in the confidentiality of its financial information is not the type of possessory interest protected by the tort of trespass to chattels.” *123 Los Robles LLC v. Metzler*, 2017 WL 10311210, \*5 (C.D. Cal. 2017) (dismissing unauthorized access claim); *Vertkin v. Vertkin*, 2007 WL 4287512, \*3 (N.D. Cal. 2007) (dismissing claim where “[t]he only harm alleged ... was a result of the information that ... procured from Plaintiff’s computers”); *Casillas v. Berkshire Hathaway Homestate Ins. Co.*, 79 Cal. App. 5th 755, 764 (2022) (trespass does not protect interests in scraped data).<sup>16</sup>

Recognizing this, X pivots, claiming in a single, conclusory sentence that Bright Data’s “acts have diminished the server capacity that X Corp. can devote to its legitimate users.” FAC ¶ 98. That does not satisfy *Twombly*. It just parrots the claim’s elements. Nor is there anything specific to Bright Data about that allegation. The same thing could be said for the most de minimis instance of unauthorized access by anyone. As one of the largest social media platforms in the

---

<sup>16</sup> Putting aside any alleged impact on X’s physical servers, X’s other articulations of its harms – interference with its “platform,” “technological infrastructure,” “software,” and “server capacity” – similarly are not trespass harms because they do not involve the touching of *tangible* property. These concepts, instead, are ethereal figments, merely reflecting a measure of computing power.

1 world, X has almost unlimited server capacity. It has not alleged that Bright Data caused X's  
2 platform to suffer any outage or server failure. Nor does X allege that its servers had to turn away  
3 other users' requests because it was too busy providing Bright Data with answers to its inquiries.  
4 The Complaint does not even attempt to back its *theoretical* claim of diminished server capacity.  
5 It does not, for example, allege that Bright Data's searches took up any specific percentage or even  
6 a substantial portion of its *massive* server capacity. Indeed, it does not even allege that X had to  
7 add server capacity because of Bright Data, which in any event may be an investment of resources,  
8 but not a *deprivation* of use. See *WhatsApp*, 472 F. Supp. 3d at 684 (no substantial interference  
9 where defendant's server requests "emulate[d] legitimate WhatsApp traffic.").

10 X's failure to allege a measurable loss is fatal to its trespass claim. On that score, the  
11 California Supreme Court's *Intel* decision controls. *Intel Corp.*, 30 Cal. 4th at 1357. There, the  
12 court rejected the argument that the defendant committed an actionable trespass by sending tens  
13 of thousands of spam emails to Intel's employees, using Intel's computer systems. As it explained:

14 "Intel ... permitted its employees to make use of [its e-mail system] both for  
15 business and, to a reasonable extent, for their own purposes.... That some  
16 [unsolicited] communications would, because of their contents, be unwelcome ...  
17 was virtually inevitable. [Defendant] did nothing but use the e-mail system for its  
18 intended purpose – to communicate with employees. The system worked as  
designed, delivering the messages without any physical or functional harm or  
disruption. These occasional transmissions cannot reasonably be viewed as  
impairing the quality or value of Intel's computer system."

19 *Id.* at 1359-60. In declining to create a "fiction of injury to the communication system," the court  
20 cited with approval cases involving the "robotic data collection," which found "insufficient  
21 evidence of harm" where there was not "obstruction of the basic function" of the plaintiffs' servers.  
22 *Id.* (citing *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 1887522, \*4 (C.D. Cal. 2000), *aff'd*,  
23 2 F. App'x 741 (9th Cir. 2001); see also *White Buffalo Ventures, LLC v. Univ. of Texas at Austin*,  
24 420 F.3d 366, 377 n.24 (5th Cir. 2005) (cautioning against courts "merely conclud[ing], without  
25 evidence or explanation, that the allegedly unauthorized use burdened the system."). Here, X's  
26 platform worked as intended; there is no trespass just because it would prefer not to receive  
27 automated server requests.  
28

VII. X FAILS TO STATE A CLAIM FOR MISAPPROPRIATION.

X’s misappropriation claim fails for the same reason: Bright Data has a right to search and use publicly available internet information. It has not “misappropriated” anything. Indeed, if Bright Data has “misappropriated” X’s property, then every business that has looked up information on the Internet has “misappropriated” information the website operator has posted to its site. A misappropriation claim cannot be stretched so far.

To state a misappropriation claim, X must allege that (i) it “invested substantial time, skill, or money in developing *its property*,” (ii) the “defendant appropriated [that] *property* at little or no cost to defendant” without “consent of plaintiff,” and (iii) the plaintiff was injured by the misappropriation of that property interest. *United States Golf Assn. v. Arroyo Software Corp.*, 69 Cal. App. 4th 607, 618 (1999). X failed to properly allege any element: it has not established a property interest in the public data Bright Data scrapes; it has not established that Bright Data misappropriated any property interest by collecting and using this public data; and it has not shown any resulting injury.

X does not say what property interest has been misappropriated.<sup>17</sup> It says it “invested substantial ... resources into the creations” of its social media platform, and that Bright Data, in contrast, has not invested its own resources into the development of the X platform. So what? A person that searches Wal-Mart.com has not invested resources in developing Wal-Mart’s retail empire, but it also has not misappropriated anything when that person tells her friend that a particular product may be on sale. That is not because Wal-Mart consented to the use and disclosure of the information, but because no *property* has been misappropriated.

---

<sup>17</sup> See *Alexander v. Metro-Goldwyn-Mayer Studios Inc.*, 2017 WL 5633407, \*6 (C.D. Cal. 2017) (“misappropriation ... claims are actionable only to vindicate legally protected *property* interests.”); *Hollywood Screentest of Am., Inc. v. NBC Universal, Inc.*, 151 Cal. App. 4th 631, 650 (2007) (“the thing misappropriated [must be] such that the court can characterize the ‘thing’ as a kind of *property right*”); *Nexsales Corp. v. Salebuild, Inc.*, 2012 WL 216260, \*4 (N.D. Cal. 2012) (same; dismissing common law misappropriation because plaintiff failed to allege any misappropriated *property* that would not be duplicative of its trade secret claim); *Cap. Credit All., Inc. v. Lowpay, Inc.*, 2008 WL 2513692, \*2 (D. Nev. 2008) (rejecting misappropriation claim because plaintiff failed to allege misappropriation of “*property*” even though they “no doubt invested substantial ‘time, effort and money’ into their business.”).



1 So too, Bright Data has not misappropriated the X platform. It has not created a clone of  
 2 the X platform using X's servers, renaming it "Twitter 2 brought to you by Bright Data." Bright  
 3 Data servers simply communicated with X's servers, requesting publicly available information.  
 4 X's servers responded with answers. That is not a misappropriation of X's platform; it is a use of  
 5 the Internet. Even X seems to acknowledge this. The misappropriation allegation – appearing in  
 6 paragraph 110 – makes no mention of any appropriation of the *platform*.

7 Instead, it alleges that Bright Data "appropriated" the "data" made available on its websites.  
 8 FAC ¶ 110. But X does not claim a property interest in this data. It does not claim title to the  
 9 information; it does not say the information is protected by copyright interest, the "hot news"  
 10 doctrine, or trade secret. Indeed, if the data belongs to anyone, it would be the original creators of  
 11 the content who used X as the *publisher* – not the author – of the content. This is confirmed by  
 12 X's own Terms, which state, "You" – the user – "retain your rights to any Content you submit,  
 13 post or display on or through [X]... What's yours is yours." Ex. 1 § 3. Nor did X spend time,  
 14 money, or effort in creating this data; the users who authored the tweets did.<sup>18</sup>

15 The breadth of X's property grab is extraordinary. Facts and figures in a database are not  
 16 protected by copyright. If a database creator wants to protect that information, it can do so through  
 17 contract or trade secret (if applicable), or by putting the information behind a log-in. Indeed, that  
 18 is how Westlaw protects its investment in creating searchable legal databases. But the database  
 19 creator does not become the *owner* of the data just because it spent some time to assemble it. If  
 20 the database creator chooses to make that data publicly available – unprotected by copyright, trade  
 21 secret, or contract – common law misappropriation will not create a fictional property right.  
 22 *Gannett Satellite Info. Network, Inc. v. Rock Valley Cmty. Press, Inc.*, 1994 WL 606171, \*5 (N.D.  
 23 Ill. 1994) (no misappropriation where "defendant's use of the quoted material occurred only after  
 24

---

25 <sup>18</sup> Indeed, any misappropriation based on the underlying data would be pre-empted by Copyright.  
 26 See *Barclays Cap. Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876, 902 (2d Cir. 2011)  
 27 (misappropriation claim pre-empted where news aggregator was merely "collecting, collating and  
 28 disseminating factual information" financial institutions published); *Nat'l Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841 (2d Cir.1997) (same; misappropriation claim for re-publication of basketball statistics pre-empted).

1 plaintiff had already published its newspaper articles”).<sup>19</sup>

2 Even if X could identify a non-pre-empted property interest, it cannot establish lack of  
3 consent. As with trespass, the consent to send and receive electronic communications over the  
4 Internet emanates from X’s participation in the World Wide Web. Absent some enforceable  
5 contract, a website operator has no right to tell other Internet users what requests their servers can  
6 and cannot make. A homeowner cannot prevent a telemarketer from asking if he or she is  
7 interested in buying life insurance, even if her phone number is on the Do Not Call Registry. It  
8 does not matter that the homeowner invested “resources” in installing the phone line, and that the  
9 telemarketer did not. There is no misappropriation of the phone line; only consensual use of a  
10 communications network by both parties to the conversation. The misappropriation claim fails.

#### 11 **VIII. X FAILS TO STATE A CLAIM UNDER THE UCL.**

12 California’s unfair competition law does not prohibit the scraping of public websites.  
13 Scraping is not illegal, and nothing in the UCL makes it so.

14 The UCL prohibits three distinct categories of conduct: “unlawful, unfair, and fraudulent  
15 business acts.” Cal. Bus. & Prof. Code § 17200. X brings claims under the “unlawful” and  
16 “fraudulent” prongs, but not the “unfair” prong. And for good reason. If scraping of public  
17 information were “unfair,” then the Internet as we know it would not exist, since everyone who  
18 has ever typed a query into a search engine has made use of automated scraped data.

19 Instead, X asserts that Bright Data violated the UCL because Bright Data’s conduct  
20 “constitute[s] trespass and tortious interference with business relationships in violation of the law.”  
21 FAC ¶ 104. But this “UCL bootstrap” fails for the same reasons the underlying tortious  
22 interference and trespass claims fail. *Woods v. Google Inc.*, 2011 WL 3501403 (N.D. Cal. 2011)  
23 (dismissing UCL claim where predicate claims also failed). No more needs to be said about that.

---

24  
25 <sup>19</sup> In *hiQ Labs, Inc. v. LinkedIn Corp.*, 2021 WL 1531172, \*8 (N.D. Cal. 2021), the court took an  
26 expansive view of common law misappropriation, suggesting that California courts would not  
27 require allegations of “direct competition between plaintiff and defendant.” But the court did not  
28 address Copyright pre-emption. To the extent *hiQ* holds that the copying of *public* web data  
hosted, but not owned by, a social media platform host rises to a non-pre-empted claim of  
“misappropriation,” it is wrongly decided.

1 X next says Bright Data committed fraud by operating a proxy network. But proxy  
2 networks are not frauds. X has not alleged misrepresentation of a single *fact*. That renders its  
3 claim procedurally and substantively deficient. Procedurally, X failed to plead fraud with  
4 particularity. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009) (Rule 9(b)  
5 applies to UCL claim sounding in fraud).

6 Substantively, X only alleges that Bright Data operates a proxy network with rotating IP  
7 addresses. But proxy networks are not illegal or fraudulent. Almost everyone at times masks their  
8 IP address and browses anonymously. For example, when employees connect through their  
9 employers' VPN, their IP addresses are masked. This might mask the actual user, but it does not  
10 render the search illegal. Nor does the use of rotating IP addresses turn Bright Data into a fraudster.  
11 The IP addresses are real; there is no lie, just because X can't tell who is using them.

12 At most, X complains that Bright Data anonymizes the user. So what? Anonymization is  
13 not fraud. *Nothing* requires an internet user to reveal his or her identity. Otherwise, Google would  
14 be in handcuffs for its Chrome browser's Incognito mode, and anyone who uses it, or a VPN, or  
15 even a library computer would be liable under the UCL. That is not the law.

16 Nor can intent change the outcome. One does one have to look to the modern age to see  
17 this is so. If anonymization were fraudulent, then undisclosed principals would be illegal, and  
18 broad swaths of the Restatement of Agency dealing with such relationships would not exist.  
19 Certainly, a business seeking to build a new plant can purchase parcels of land anonymously before  
20 prices skyrocket. When sellers find out about the development plan, they may be sorry they didn't  
21 hold out for more, but they cannot sue in fraud. Anonymity is fine.

22 At most, X's complaint – that neither Bright Data nor its users identify themselves – is an  
23 omitted fact. But an omission is not a misrepresentation unless there is first "a duty to disclose."  
24 *Hodsdon v. Mars, Inc.*, 891 F.3d 857 (9th Cir. 2018). There is no duty here. X does not claim that  
25 Bright Data is a fiduciary, and the rules of the Internet do not require everyone to append their  
26 name to their searches. Website operators, of course, sometimes do require users to disclose their  
27 identity, such as by asking users to log-in. If website operators do that, they can use the UCL or  
28

1 the Computer Fraud and Abuse Act to guard against evasion of the log-in. And if X had done that  
2 here, it could track their users with Orwellian accuracy, knowing for certain who visited the  
3 platform, how much time they spent on each page, and what they searched, regardless of whether  
4 they used Bright Data's proxy network or not. X *chose* not to. Instead, it chose to operate a virtual  
5 public town square, allowing anyone with an internet connection to visit. It did not turn away  
6 those that chose to remain anonymous. That was a choice. But having made that choice, X cannot  
7 now sue Bright Data in fraud because its new owner – Mr. Musk – regrets having done so.

8 **IX. X'S INDIVIDUAL USER ACCOUNT CLAIMS SHOULD BE DISMISSED.**

9 Once X put Bright Data on notice of its claims, Bright Data terminated its corporate  
10 accounts. This precludes any liability for forward-looking conduct based on these accounts. But  
11 Bright Data cannot fire every employee that has an X account. Recognizing this, X appears to  
12 base its contract claim on the fact that “several of [Bright Data's] executives ...[,] employees[,] and agents” also have individual X accounts. FAC ¶¶ 42-43, 80. But the mere fact that a Bright  
13 Data employee has an X account cannot bind Bright Data.  
14

15 Virtually every company in the world has at least one employee with an X account, but not  
16 every company is contractually bound to X. Nor can employees' X accounts be used to impute  
17 knowledge of the Terms to every company. X alleges only that some Bright Data employees “are  
18 also registered X users and [themselves] expressly agreed to X Corp.'s Terms when registering  
19 their accounts.” FAC ¶¶ 42, 43. But X is not bringing any claims against any Bright Data  
20 employee, or based on any alleged agreement with a Bright Data employee. To bind Bright Data  
21 through its employees' individual accounts, X must plead facts showing that Bright Data is, in  
22 fact, a party to the user agreement between the individual and X. This X does not do.

23 X identifies seven individual accounts opened by current or former Bright Data employees.  
24 See FAC ¶¶ 42-43. But there is no allegation that these accounts were owned, controlled, or  
25 managed by Bright Data, or opened on its behalf. As X alleges, each account was opened in the  
26 individual's name, not Bright Data's. See *id.* Nor does X allege that these individuals were acting  
27 in their capacities as Bright Data employees when opening these accounts. Indeed, X does not  
28

1 even allege that these individuals *were* employed by Bright Data when they opened their personal  
2 accounts.<sup>20</sup> Nor does X allege that these accounts were used for the scraping activities at issue.  
3 Put simply, other than employment at Bright Data, nothing distinguishes these accounts from any  
4 of the millions of X accounts opened by random people everywhere.

5 Both contract and agency law preclude liability, or imputing knowledge, from these  
6 individual accounts. As to contract law, the Court need only look at the Terms themselves:

7 “If you *are accepting these Terms and using the Services on behalf of a company*  
8 ..., you represent and warrant that you are *authorized to do so and have the*  
9 *authority* to bind such entity to these Terms.” Ex. 1 § 1.

10 Thus, an employer is not bound unless the employee (i) has “the authority” to create and use  
11 accounts on behalf of the company; (ii) actually opens the account “on behalf of a company;” and  
12 (iii) “us[es] the Services on behalf of” the company.” *Id.* None of these conditions are alleged.

13 Agency law confirms. Respondeat superior in tort does not apply because X does not seek  
14 to hold Bright Data liable for the acts of any individual employee. *See* Restatement (Third) Of  
15 Agency § 2.04 (“An employer is subject to liability *for torts* committed by employees while acting  
16 within the scope of their employment.”).

17 Rather, X seeks to satisfy contract formation by asserting these individual accounts  
18 constitute *assent* by Bright Data. But these accounts do not purport to be on behalf of Bright Data  
19 and were instead created solely for the employees’ benefit. This precludes holding Bright Data  
20 liable under contract or imputing Bright Data’s knowledge of the Terms based on its employees’  
21 individual accounts. *See* Rest. 3d Agency § 6.03, cmt. c (“An undisclosed principal only becomes  
22 a party to a contract when an agent acts on the principal’s behalf in making the contract.”).  
23

---

24 <sup>20</sup> This is no mere oversight. A LinkedIn search shows most X accounts pre-date their owners’  
25 association with Bright Data. Erez Naveh allegedly had a Twitter account “since at least August  
26 2009,” but only joined Bright Data in April 2022. Or Lechner had an account since “December  
27 2012,” but only joined in late 2015. Yanay Sela had an account since “December 2014,” but only  
28 joined in 2021. Omri Orgad had an account since “November 2011,” but only joined in 2014.  
Zachary Keyser had an account since “December 2019,” but only joined in November 2021.  
Artem Shibakov had an account since “February 2013,” but only joined in June 2021.

**X. CONCLUSION.**

For the foregoing reasons, the Court should dismiss the Amended Complaint.

1 Dated: December 13, 2023

Respectfully submitted,

2  
3 /s/ Colin R. Kass

4 Colin R. Kass\*  
5 PROSKAUER ROSE LLP  
6 1001 Pennsylvania Ave., N.W.  
7 Washington, D.C. 20004  
8 (202) 416-6890  
9 ckass@proskauer.com

10 David A. Munkittrick\*  
11 PROSKAUER ROSE LLP  
12 Eleven Times Square  
13 New York, New York 10036  
14 (212) 969-3000  
15 dmunkittrick@proskauer.com

16 Robert C. Goodman (Bar No. 111554)  
17 Lauren Kramer Sujeeth (Bar No. 259821)  
18 ROGERS JOSEPH O'DONNELL, PC  
19 311 California Street, 10th Floor  
20 San Francisco, CA 94104  
21 (415) 956-2828  
22 rgoodman@rjo.com  
23 lsujeeth@rjo.com

24 Sehreen Ladak (Bar No. 307895)  
25 PROSKAUER ROSE LLP  
26 2029 Century Park East, Suite 2400  
27 Los Angeles, CA 90067-3010  
28 (310) 284-5652  
sladak@proskauer.com

*Attorneys for Defendant Bright Data Ltd.*  
*\*Admitted Pro Hac Vice*